Tom and Leslie Case Report

CIS330

Examiner: Xiang Liu

Apr 30, 2023

EVIDENCE

1.Information showing Tom and Leslie’s romance.

2.Information showing Tom’s excitement at the prospect of getting promoted.

3.Information showing Tom’s concerns.

4.Tom logging on to his system and accessing other computers after hours.

5.Information showing his meeting with Mr. Melonis of Saspah Software.

6.Evidence showing Tom copying files from the server to his computer and what he

did with the files.

7.Leslie’s computer accessed files that were never on her computer from a USB drive.

8.Leslie browsing the Internet for vacation deals.

9.Information about how Tom and Leslie felt that the company owes them.

10.Evidence showing Leslie coping files containing company account numbers.

11.Information showing discussions about how they might use the accounts.

12.Leslie searching for embezzlement schemes on the Internet.

13.Leslie e-mailing Tom links she found on the Internet.

14.Leslie creating a second set of “books” (the Excel spreadsheets).

Notes for viewing this report:

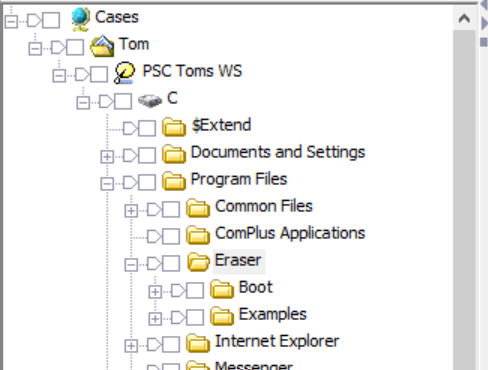
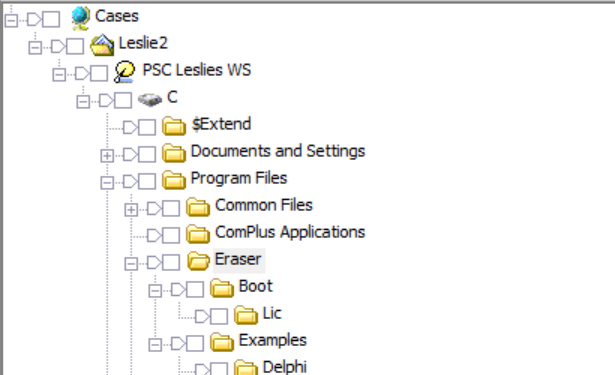
* Each evidence is separated by black lines like this: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Each evidence is explained in parenthesis and in text color blue like this:

(Tom emails Leslie on September 01, 2004)

* Evidence for example, that shows Leslie and Tom’s romance + Tom’s excitement of getting promoted will be shown like this:

(Evidence 1, Evidence 2)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(Eraser program found in both Leslie and Tom’s computers under Program Files. Eraser is a file erasure tool that is anti-forensic as it makes some data irrecoverable)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-----Original Message-----  
 **From:** Tom Warner  
 **Sent:** Wednesday, September 01, 2004 11:17 AM  
 **To:** Leslie Stowle  
 **Subject:** Lunch

Do you want to meet for lunch today?

Tom

(Tom emails Leslie on September 01, 2004 11:17 AM, asking her if she wants to meet for lunch)

(Evidence 1)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-----Original Message-----  
 **From:** Tom Warner  
 **Sent:** Thursday, September 30, 2004 10:55 AM  
 **To:** Leslie Stowle  
 **Subject:** Vice Pres

Hay Leslie,

Did you see the e-mail about “”MY NEW JOB” Wee I can’t wait, god knows I deserve it and I sure can use the x-tra money.

PS. Want to do lunch. Hee Hee

HD

(Tom emails Leslie on September 30, 2004 10:55 AM. Tom is excited about the new role. Tom asks Leslie to have lunch)

(Evidence 1, Evidence 2)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Oh Tom I am so proud of you. I always knew you would promote.

Yes we can do lunch Mr. VP

Leslie Stowle

Fanance Manager

Price Software Company

(Leslie responds to Tom’s previous email. She is proud of Tom and accepts to have lunch with him)

(Evidence 1)

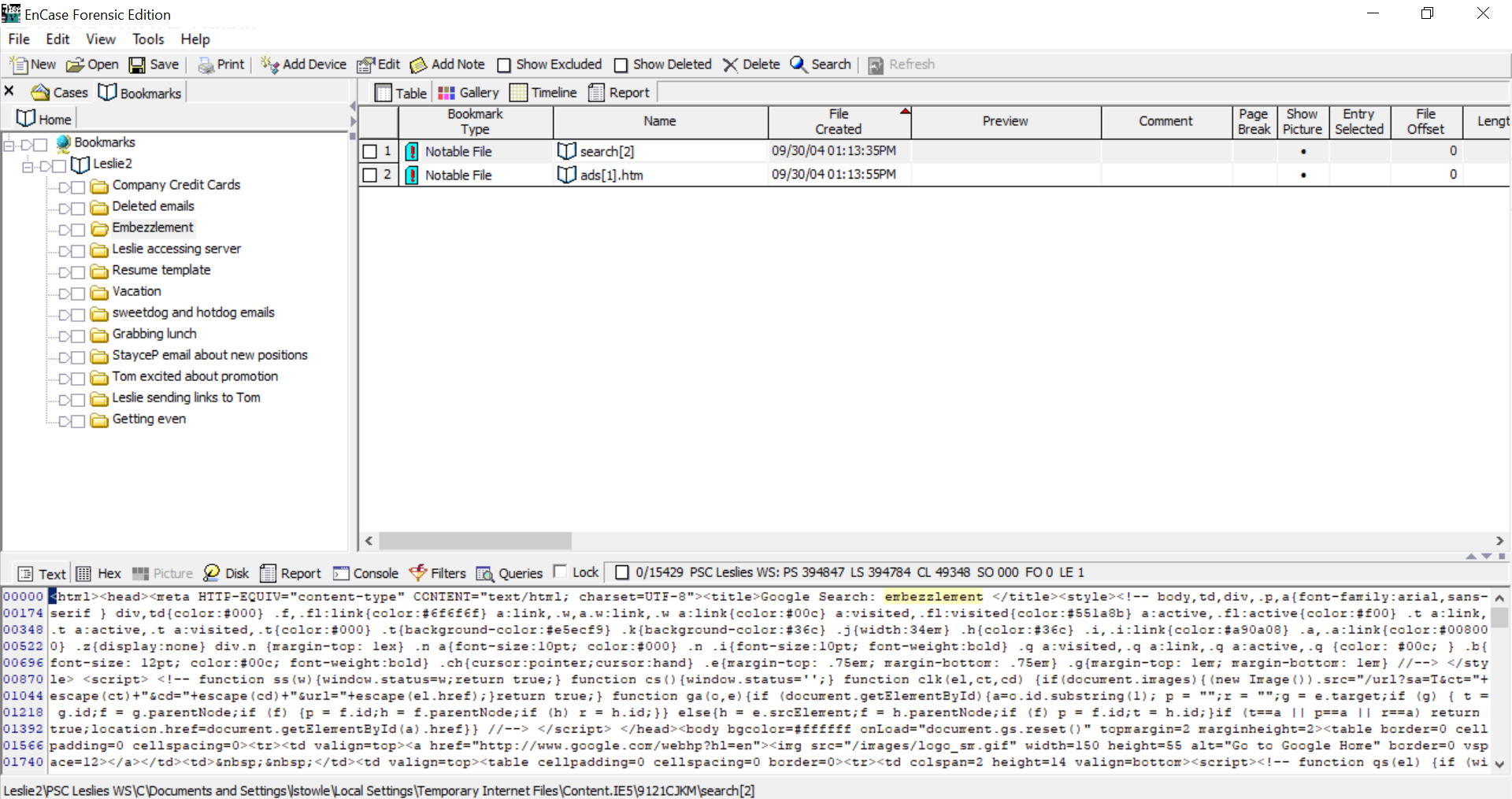
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Sure same place?

(Tom responds to Leslie)

(Evidence 1)

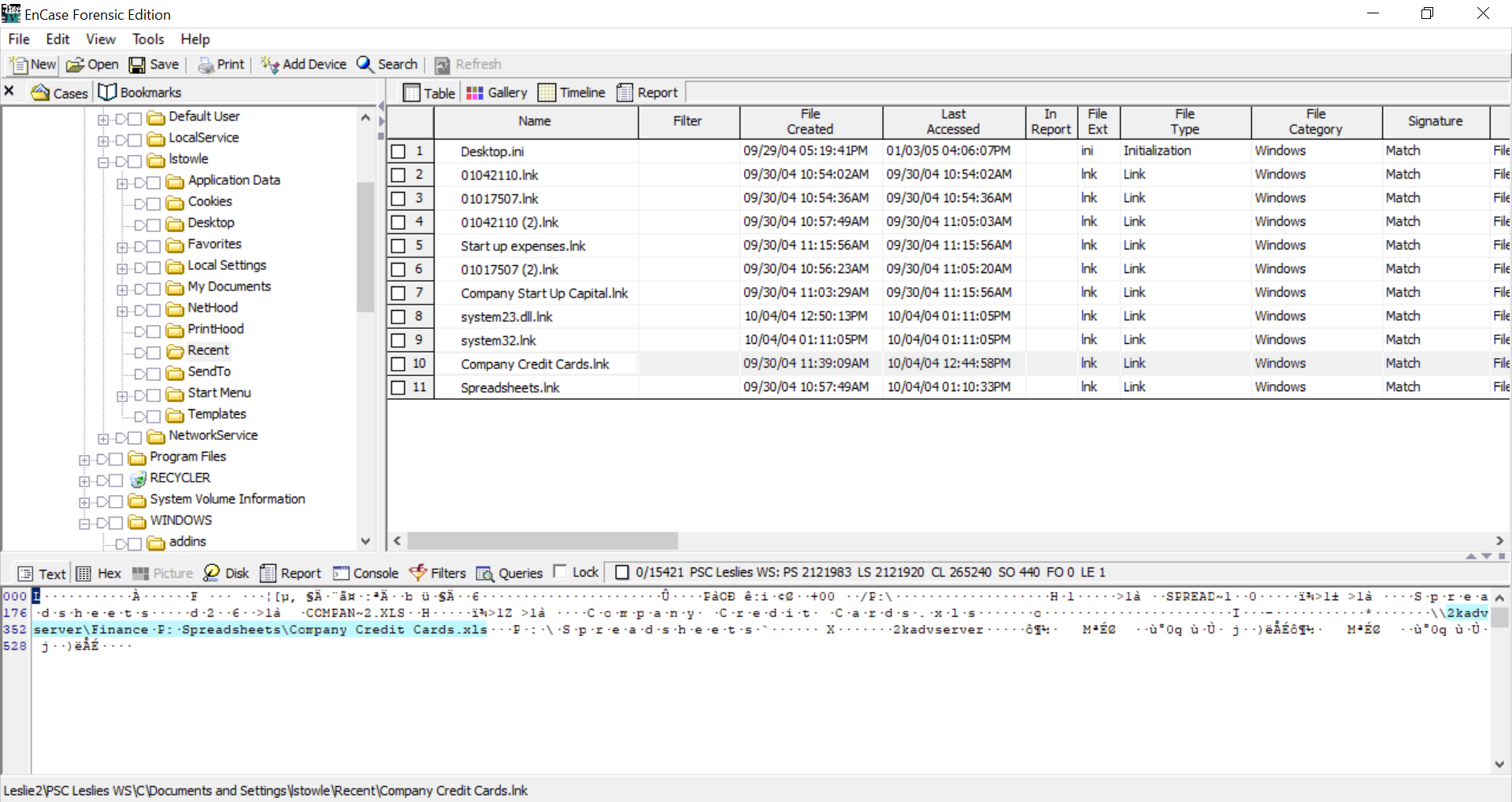
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(Leslie google searches for the term “embezzlement”, she then receives an ad for embezzlement lawyers because of her google search)

(Evidence 12)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

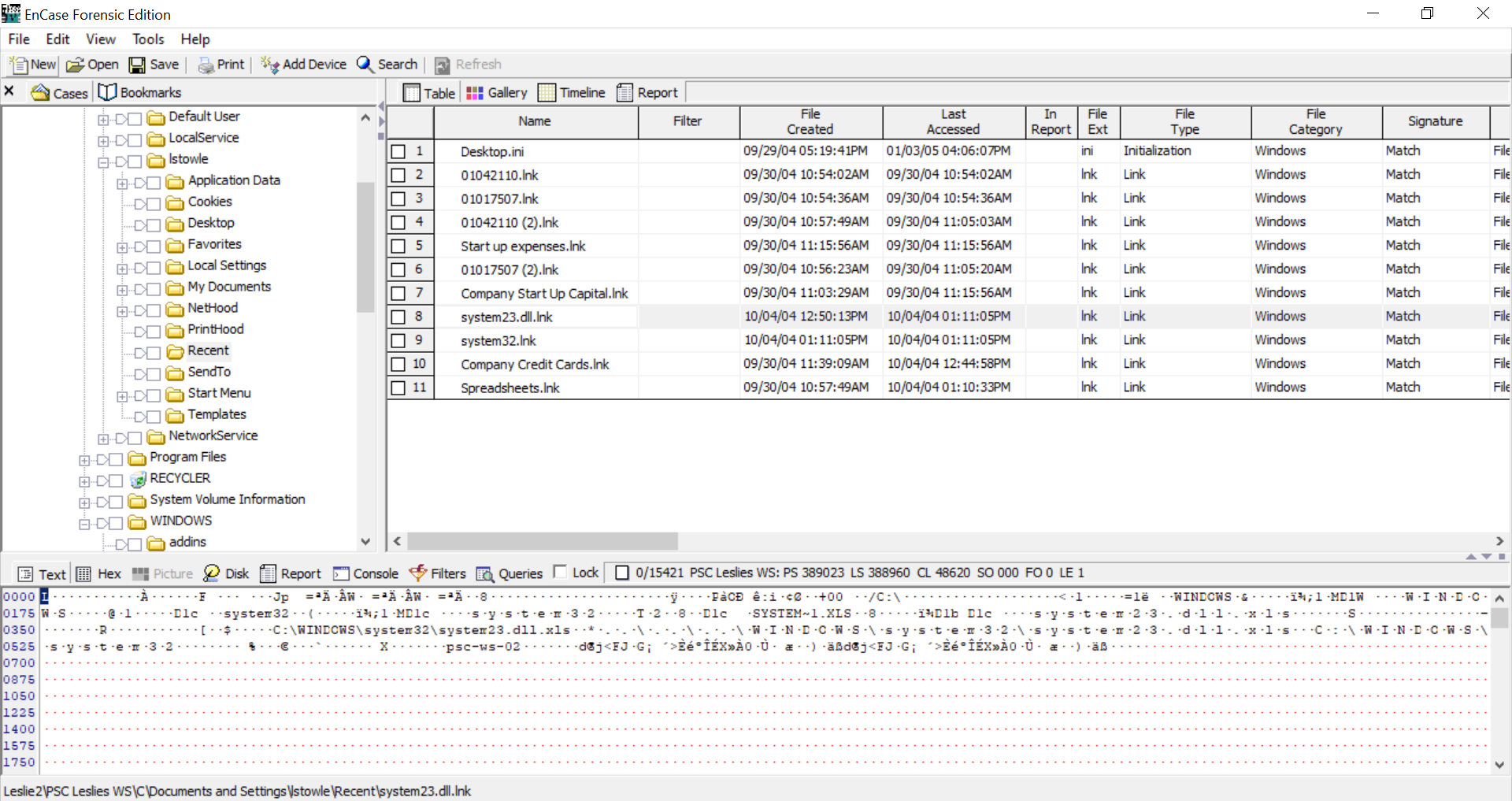


(Company Credit Cards.lnk)

(Leslie accessed the Company Credit Cards spreadsheet from the 2kadvserver. The link file is created to document her access. September 30, 2004 11:39AM link file was first created, meaning she first accessed this spreadsheet. Last accessed October 4 2004 12:44PM, meaning she last accessed it 4 days after her first access)

(Evidence 10, Evidence 14)

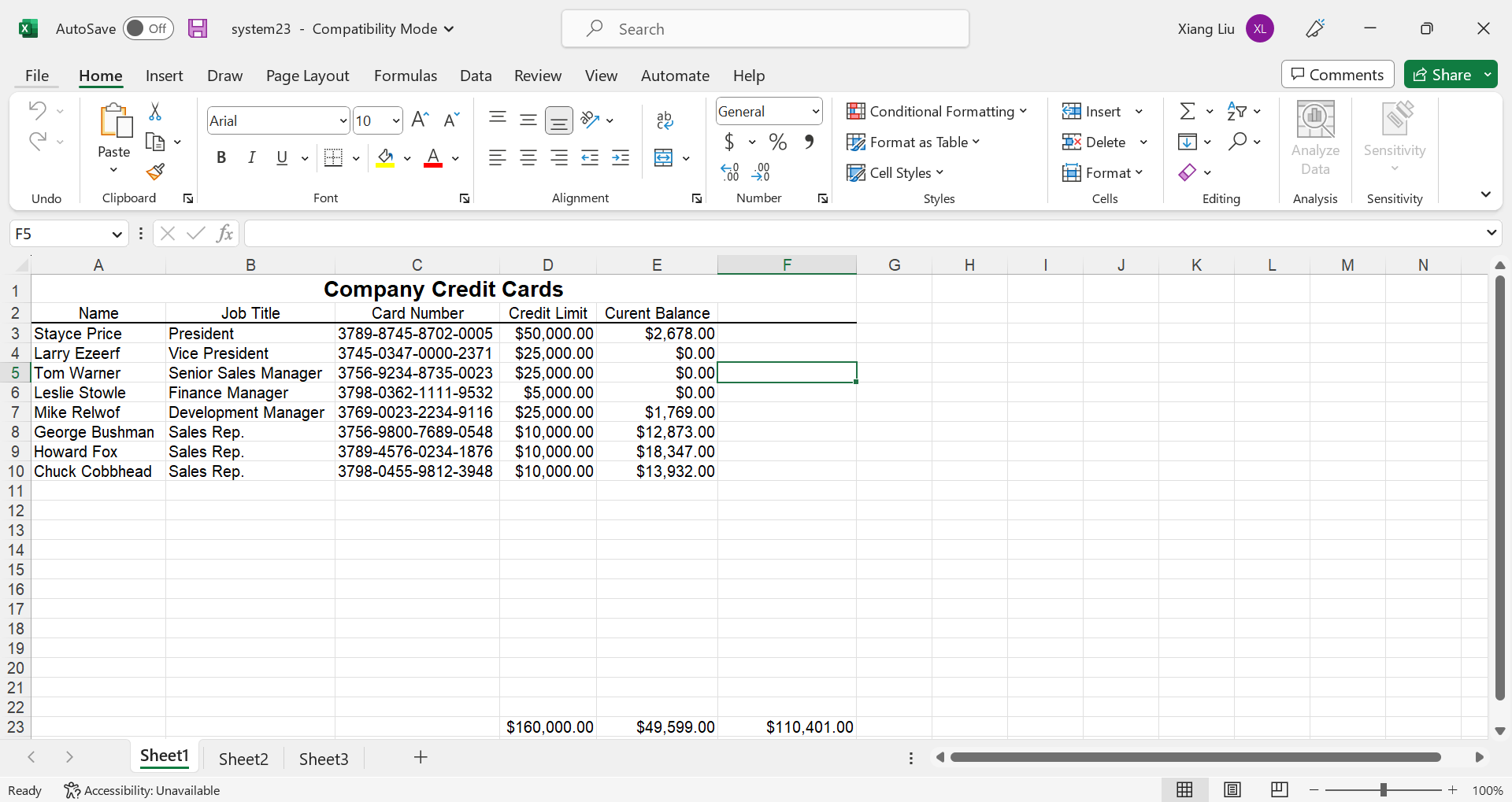
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(System23.dll.lnk)

(On October 4, 2004 12:50PM, 6 minutes after Leslie accessed the server, system23.dll.lnk was created. This contains Company Credit Card information. It was found hidden in the system32 folder on Leslie’s computer. One important part to notice is this is supposed to be a .xls file since it's an excel spreadsheet, but Leslie manually changed it to a .dll instead, trying to prevent it from being found. She hid this spreadsheet in the system32 folder and made the name system23 to disguise it with the other files.)

(Below are the contents of system23.dll)



(Showing Company Credit Card Information. Leslie most likely copied this file from the server, since the system23.dll.lnk file was created 6 minutes after she accessed the server.)

(Evidence 10, Evidence 14)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-----Original Message-----  
 **From:** Tom Warner  
 **Sent:** Thursday, September 30, 2004 11:07 PM  
 **To:** Leslie Stowle  
 **Subject:** Hay

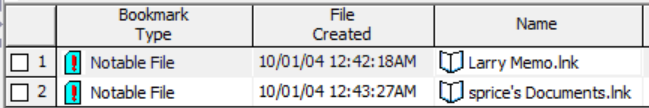
You are not going to believe this.

I found a memo that miss Price wrote that says she is not going to promote me to vice president. I will get even. Who does she think she is. I am going home now

(Tom sent Leslie an email on September 30, 2004 11:07 PM, showing his concern about losing his promotion, and his attempt to get even. “I am going home now” means Tom was most likely at work when he sent this message, after hours)

(Evidence 3, Evidence 4, Evidence 9)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(Tom accessed sprice’s documents after hours from the server, a link file was automatically created on October 1, 2004 documenting his access. This link file is created about an hour and 35 minutes after Tom sent Leslie his message about getting even, after hours)

(Evidence 4)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-----Original Message-----  
 **From:** Leslie Stowle  
 **Sent:** Monday, October 04, 2004 10:11 AM  
 **To:** Tom Warner  
 **Subject:** RE: Hay

Oh Tom, You don’t know that. Are you sure? Lets have lunch and talk about it.

Leslie Stowle

Fanance Manager

Price Software Company

(Leslie sends Tom an email on October 04, 2004 10:11 AM about the memo and getting lunch)

(Evidence 1, Evidence 3, Evidence 9)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I do know it. I saw the memo. I have proof. You don’t understand. I have been working here for 7 years. I helped start this company. They owe me so much!

No I can’t do lunch today. I have a meeting with someone. Maybe we can do dinner?

(Tom responds to Leslie’s previous email, Tom feels the company owes him)

(Evidence 1, Evidence 3, Evidence 9)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-----Original Message-----  
 **From:** Leslie Stowle  
 **Sent:** Monday, October 04, 2004 10:30 AM  
 **To:** Tom Warner  
 **Subject:** I like this one

http://www.expedia.com/pub/agent.dll?qscr=cmhi&itid=&itdx=&itty=&ecid=&from=&tpst=

Leslie Stowle

Fanance Manager

Price Software Company

(Leslie emails Tom on October 04, 2004 10:30 AM, a vacation link)

(Evidence 1, Evidence 13)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

-----Original Message-----  
 **From:** Tom Warner  
 **Sent:** Monday, October 04, 2004 10:31 AM  
 **To:** Leslie Stowle  
 **Subject:** RE: I like this one

The link does not work.

(Tom responds to Leslie on October 04, 2004 10:31 AM, saying the vacation link doesn’t work)

(Evidence 1, Evidence 13)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<http://www.expedia.com/pub/agent.dll?qscr=cmhi&htid=426160&dsct=&dlvl=&rtmn=&rtmx=&dcty=LAX&drid1=180074&tair1=KOA&ddpt1=&tdpt1=&drtn1=&trtn1=&cAdt1=2&cmbt=2&mtxt=Sample+4%2Dnight+air%2Fhotel+package+Los+Angeles+to+Big+Island+from+%241070+based+on+travel+11%2F11+through+11%2F15%2E+Sample+prices+based+on+double+occupancy+and+vary+by+dates+of+travel%2C+availability%2C+and+departure+city%2E+Shop+for+your+travel+dates+and+departure+city+below%2E&rfrr=-33440&&zz=1096910619000&>

Leslie Stowle

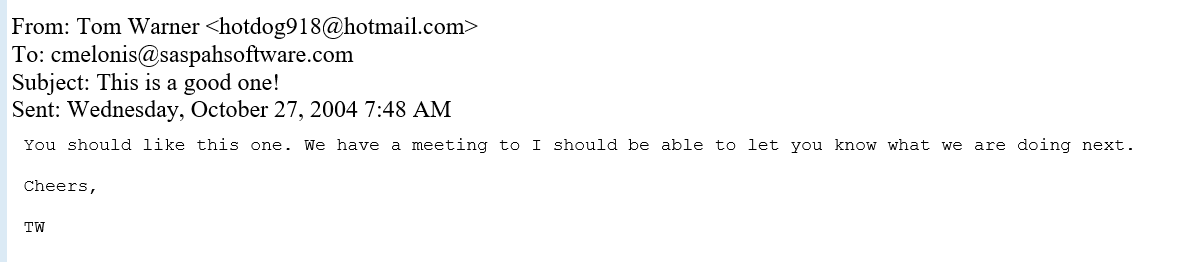
Fanance Manager

Price Software Company

(Leslie responds back to Tom with a now a working vacation link)

(Evidence 1, Evidence 13)

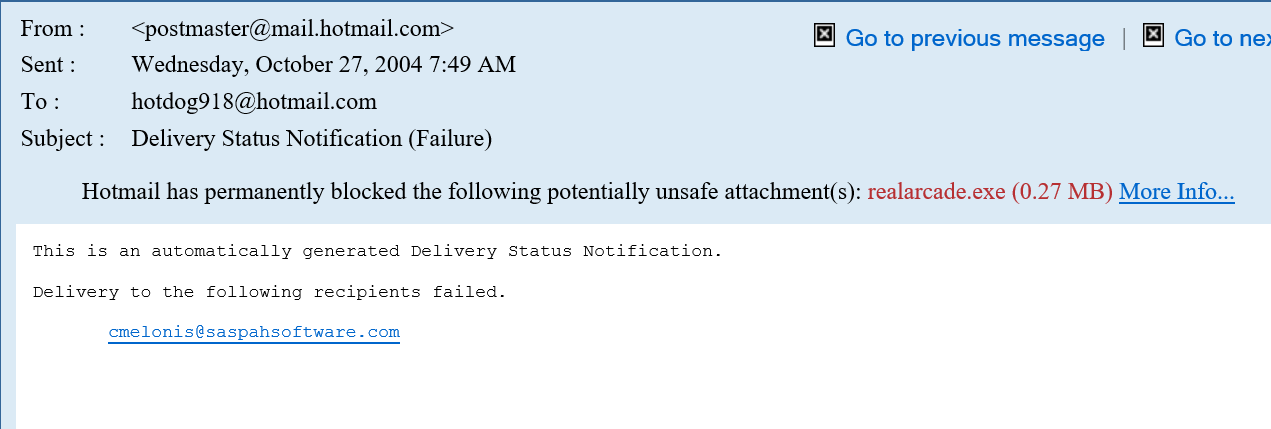
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(Tom emails Chris Melonis on October 27,2004 7:48 AM, VP of Saspah Software, PSC’s competitor, mentioning their meeting)

(Evidence 5)

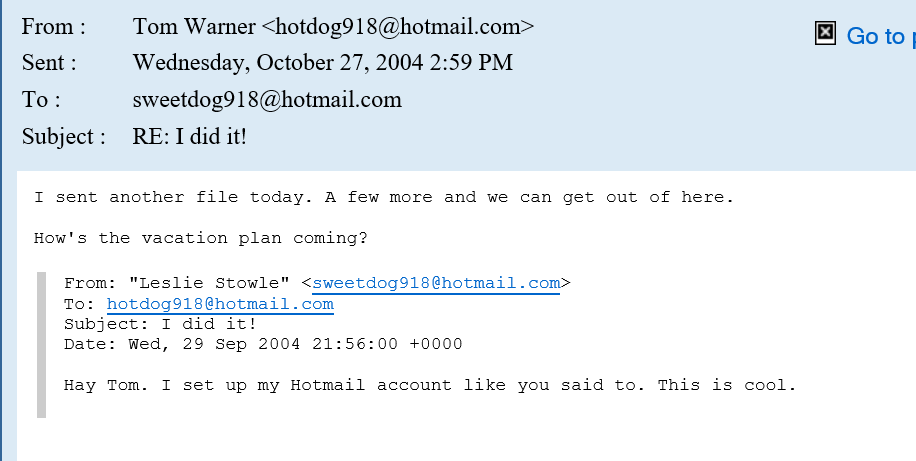
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(Tom’s previous email to Chris Melonis did not go through, because Tom attached an executable file called realarcade.exe, this postmaster is an automatic response notifying Tom that the message did not go through)

(Evidence 5)

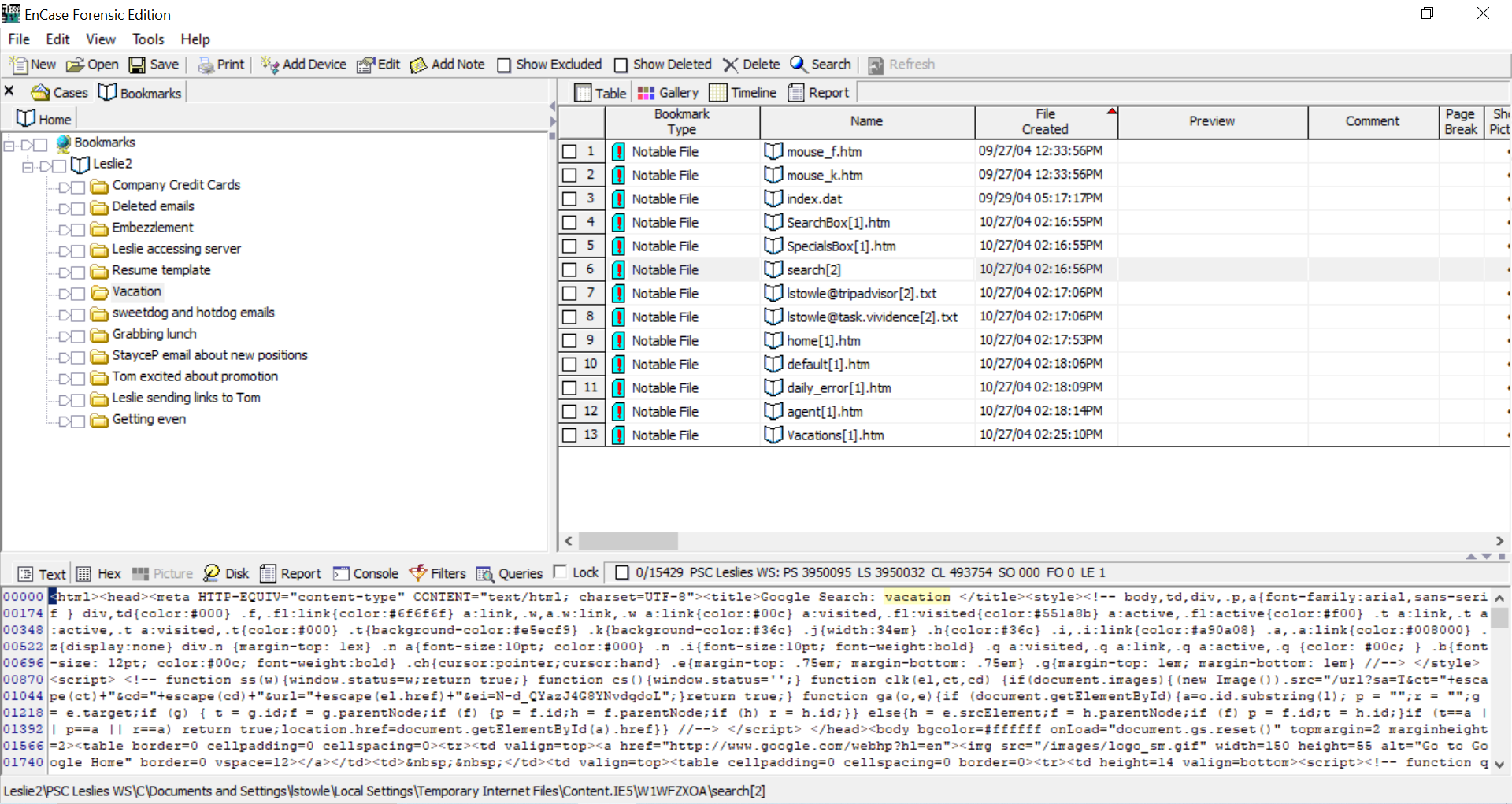
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



(Tom emails Leslie on October 27, 2004, 2:59 PM. “I sent another file today” most likely refers to realarcade.exe, the attachment that didn’t go through. Tom mentions about vacation plans with Leslie)

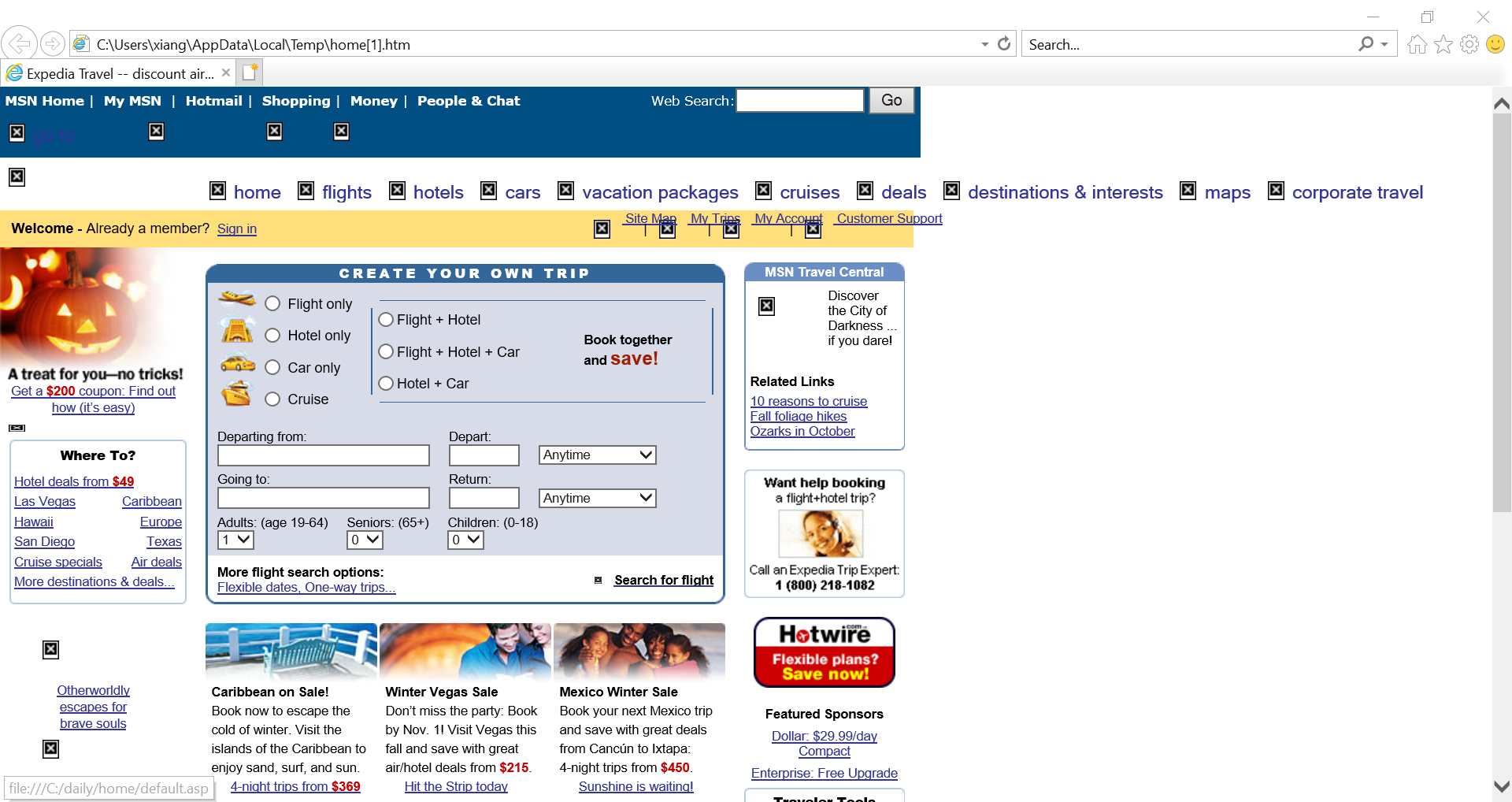
(Evidence 1, Evidence 5)

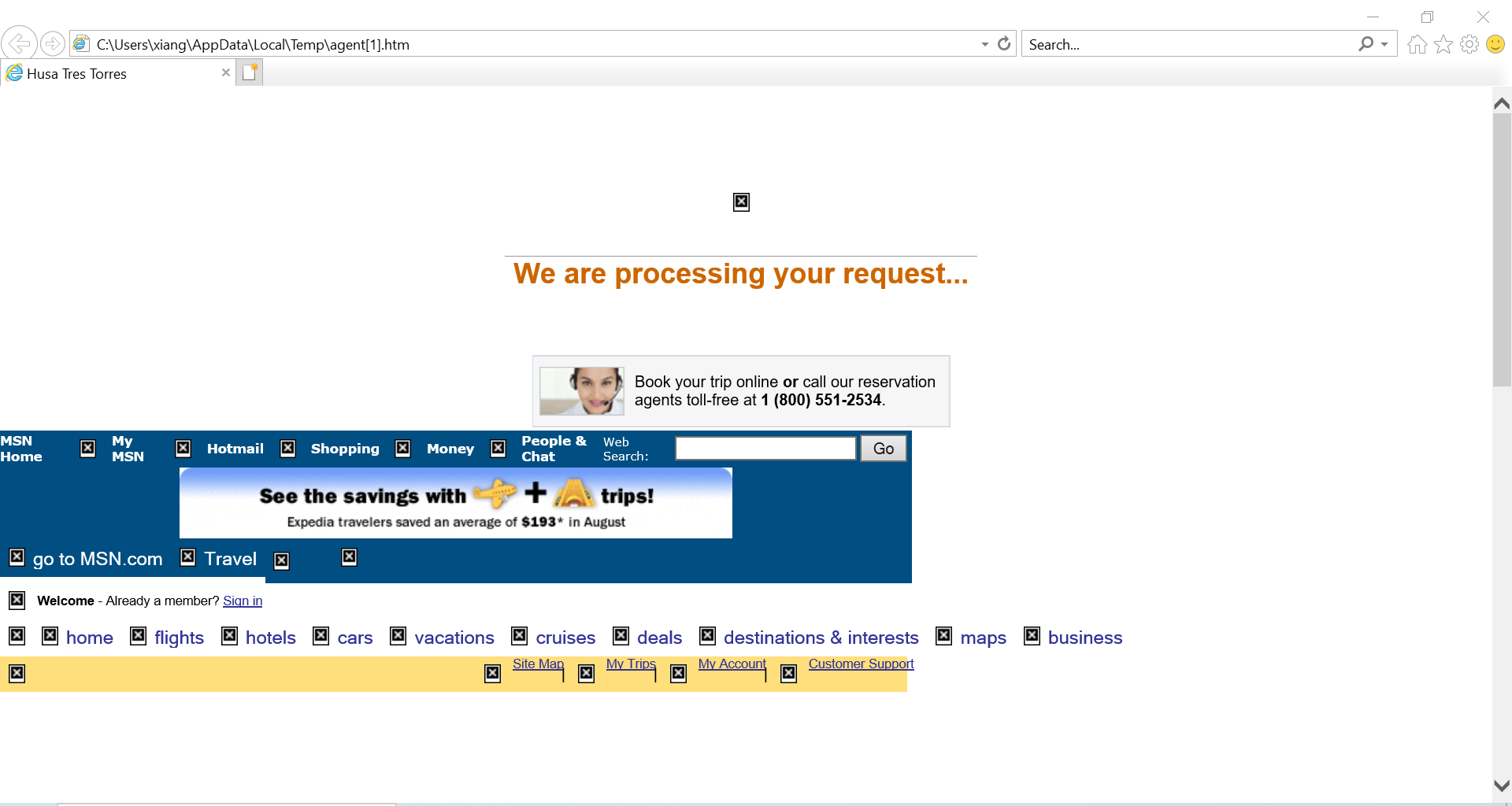
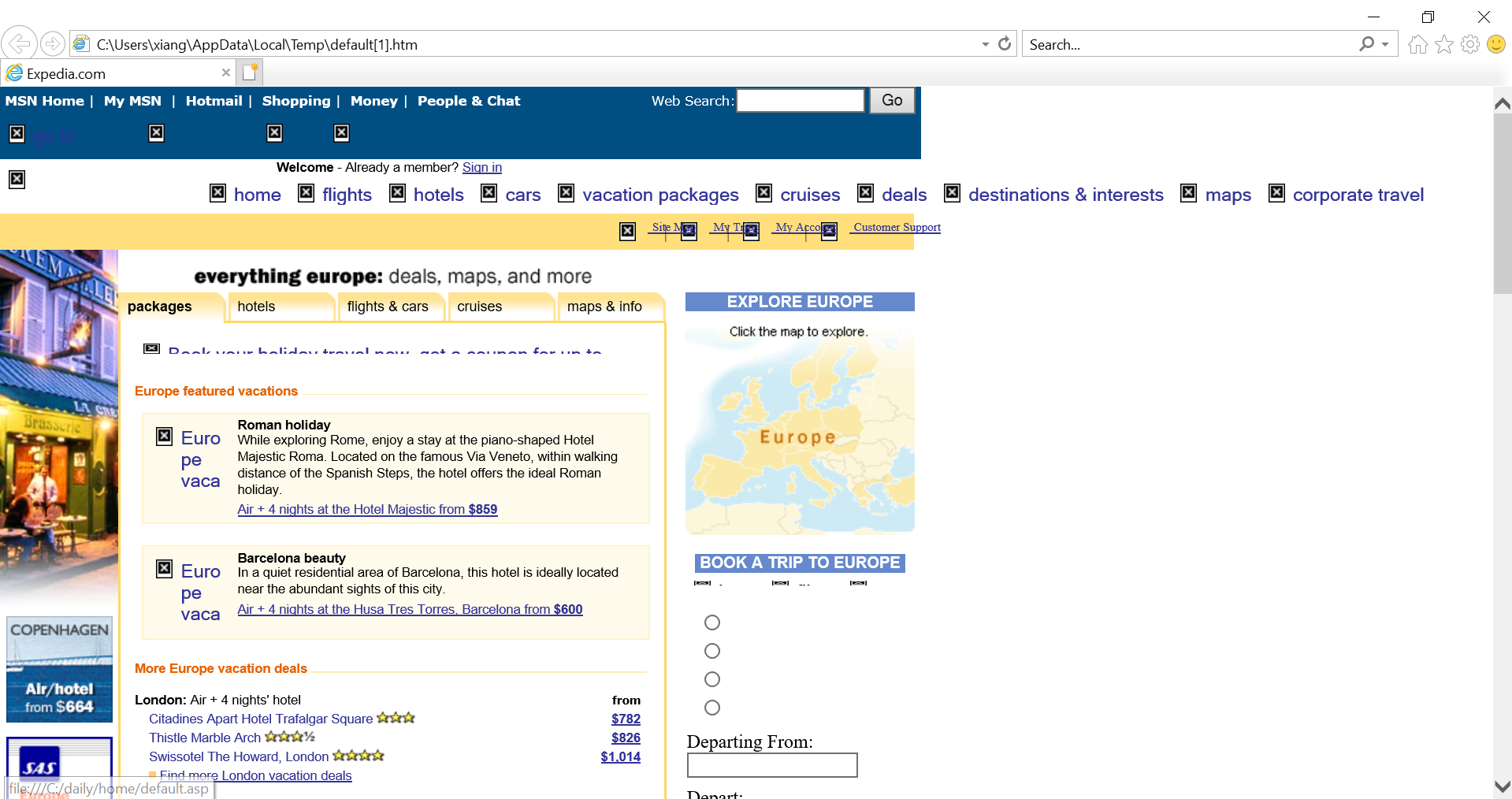
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

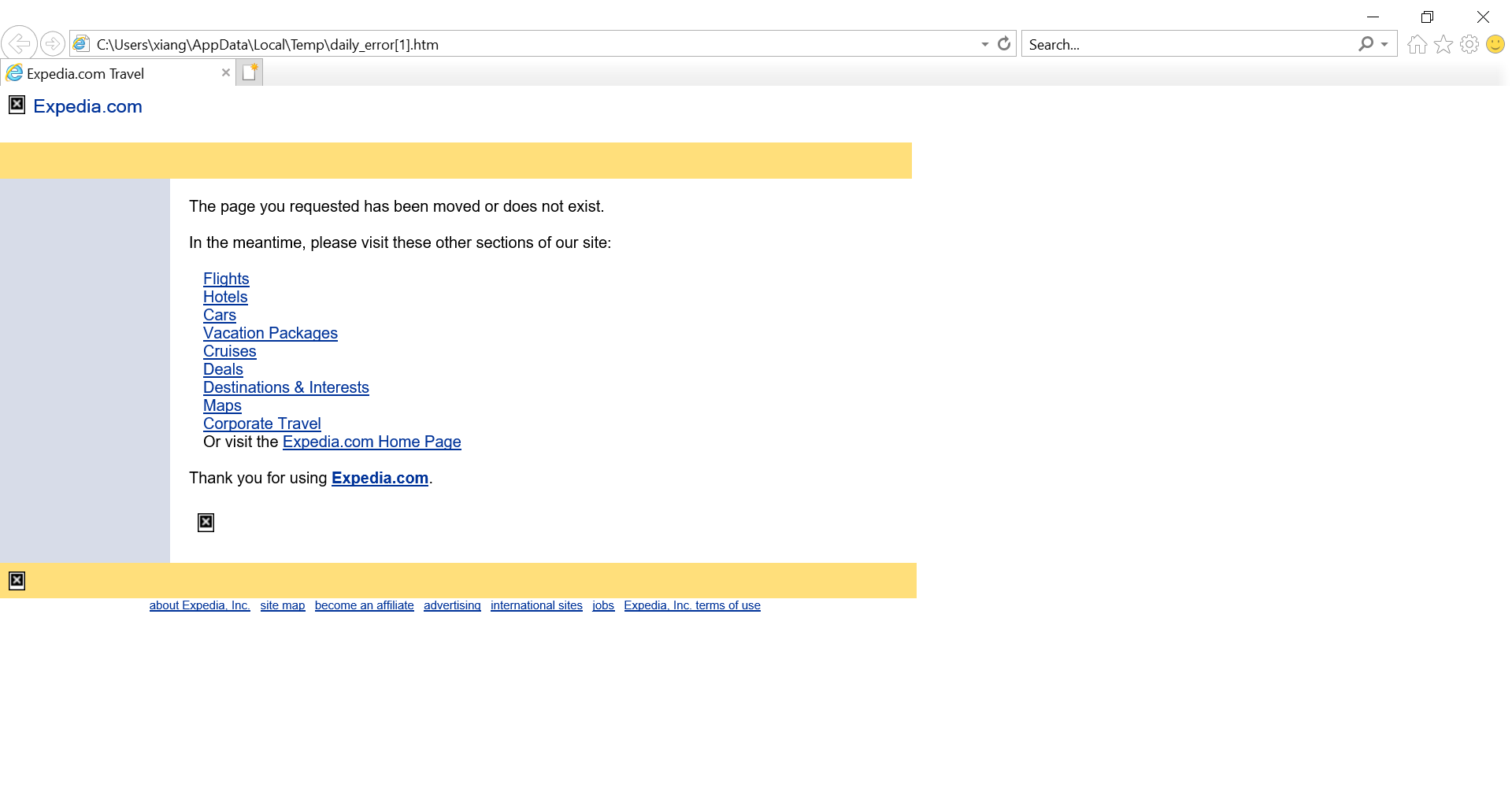


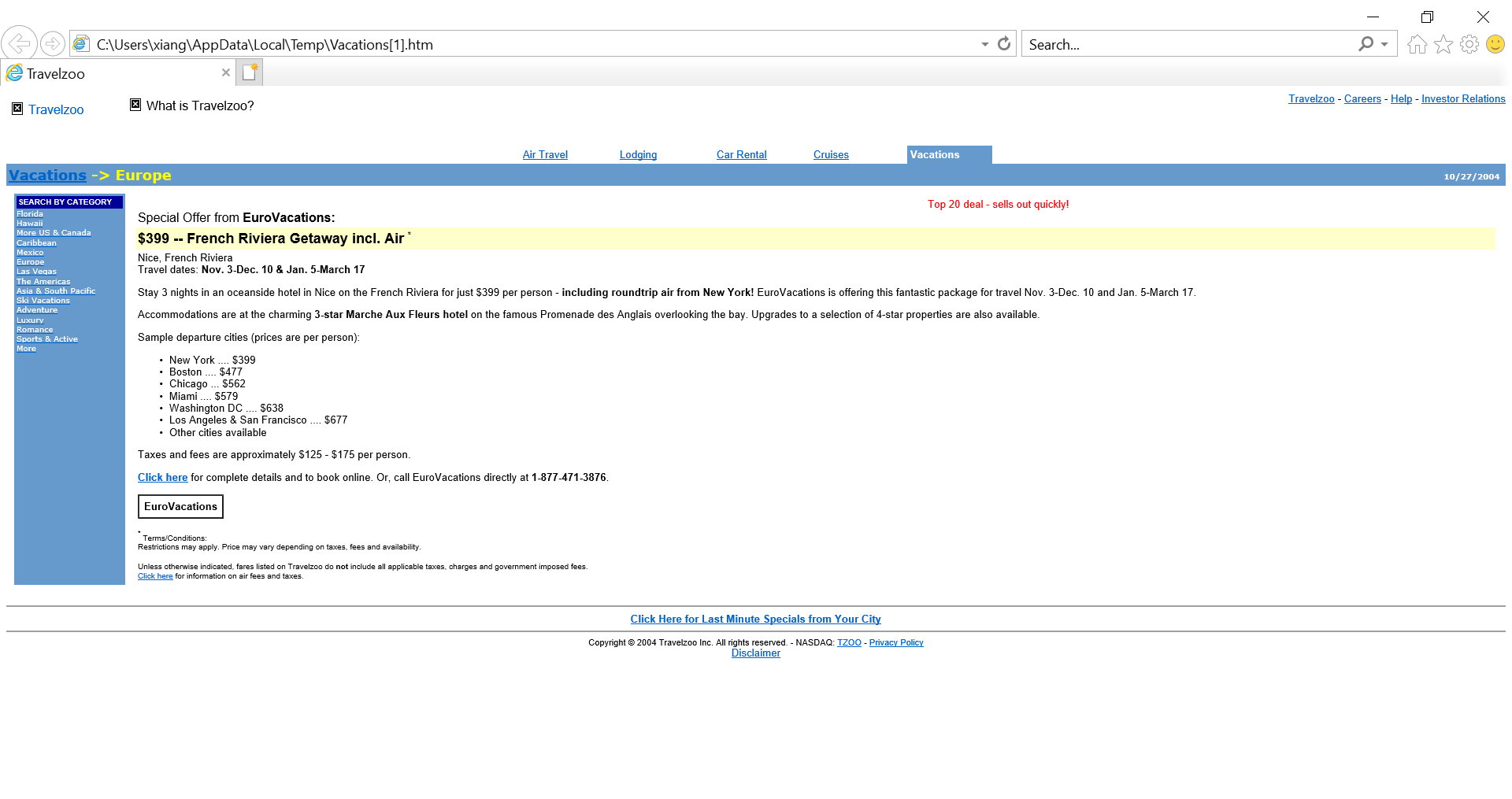
(Leslie google searches for the term “vacation” on October 27, 2004 2:16 PM. She proceeds to browse through five different websites, websites are show below)

(Evidence 8)









\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_