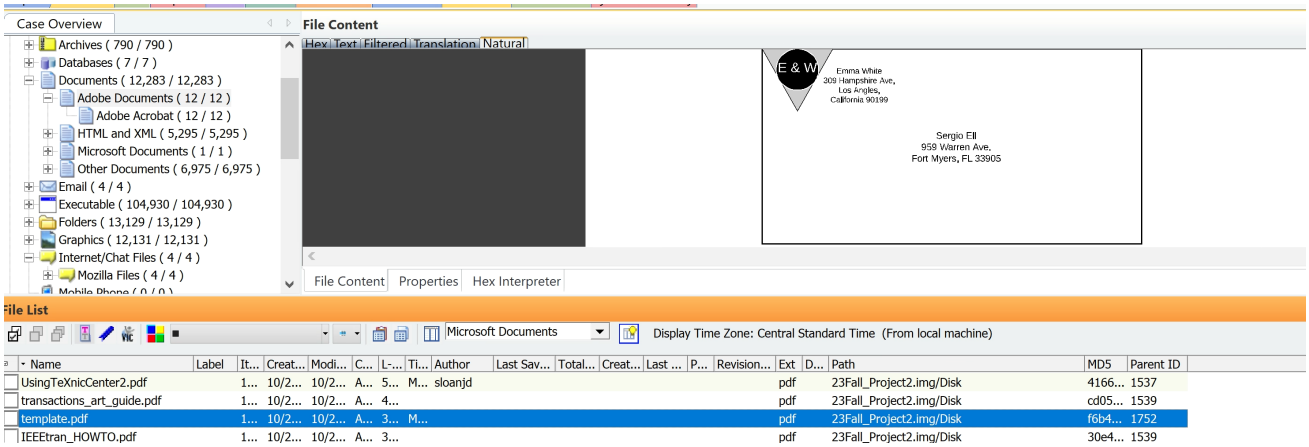
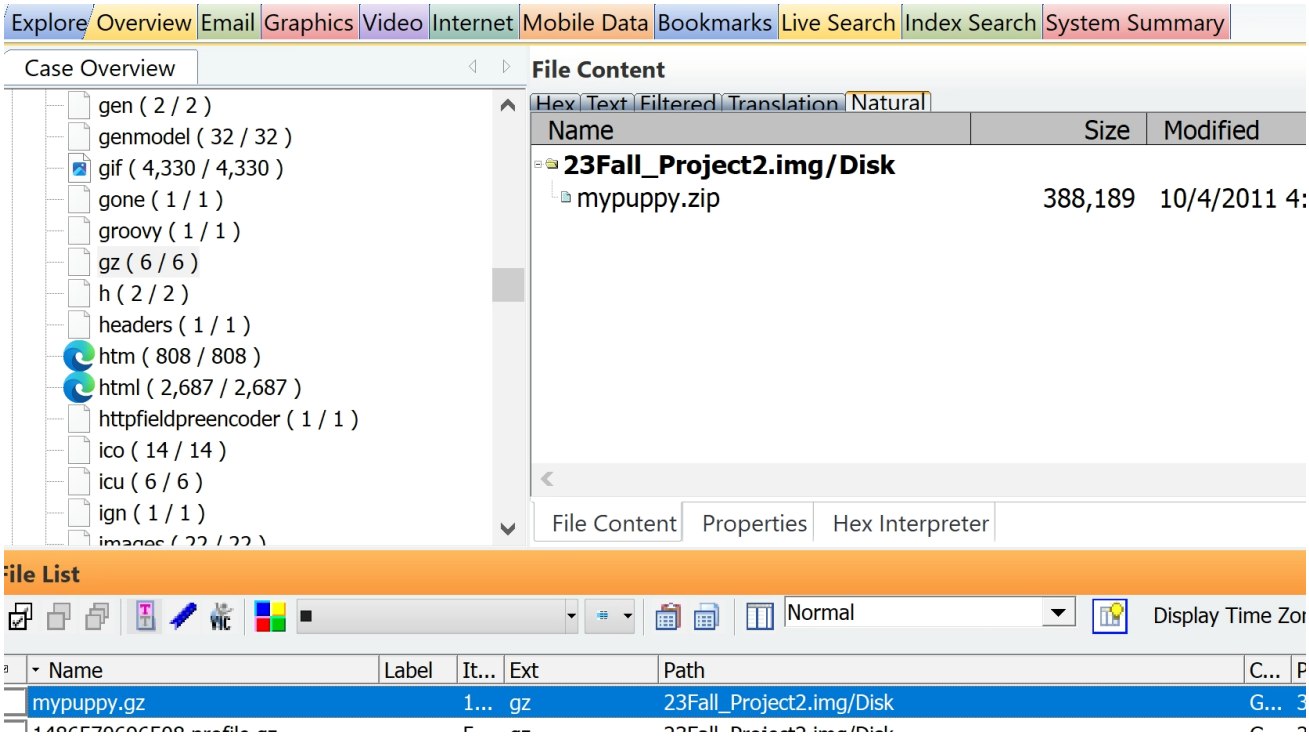
Project 2 Report

A. The suspect kept 5 figures which are the envelope labels that contain the contact information. Please find as many figures as you can.

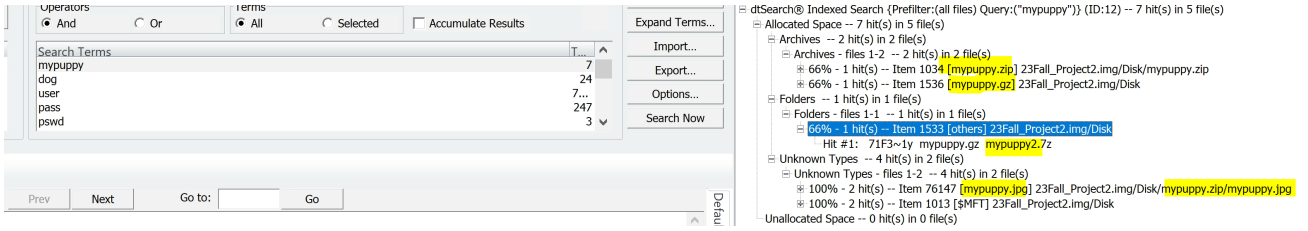
1. template.pdf - I found the first envelope by searching through the overview tab. When viewing the Adobe Document files, I found a file called manual.pdf. The last page of manual.pdf contains an envelope giving me clues about the sender like her name or alias, Emma White.



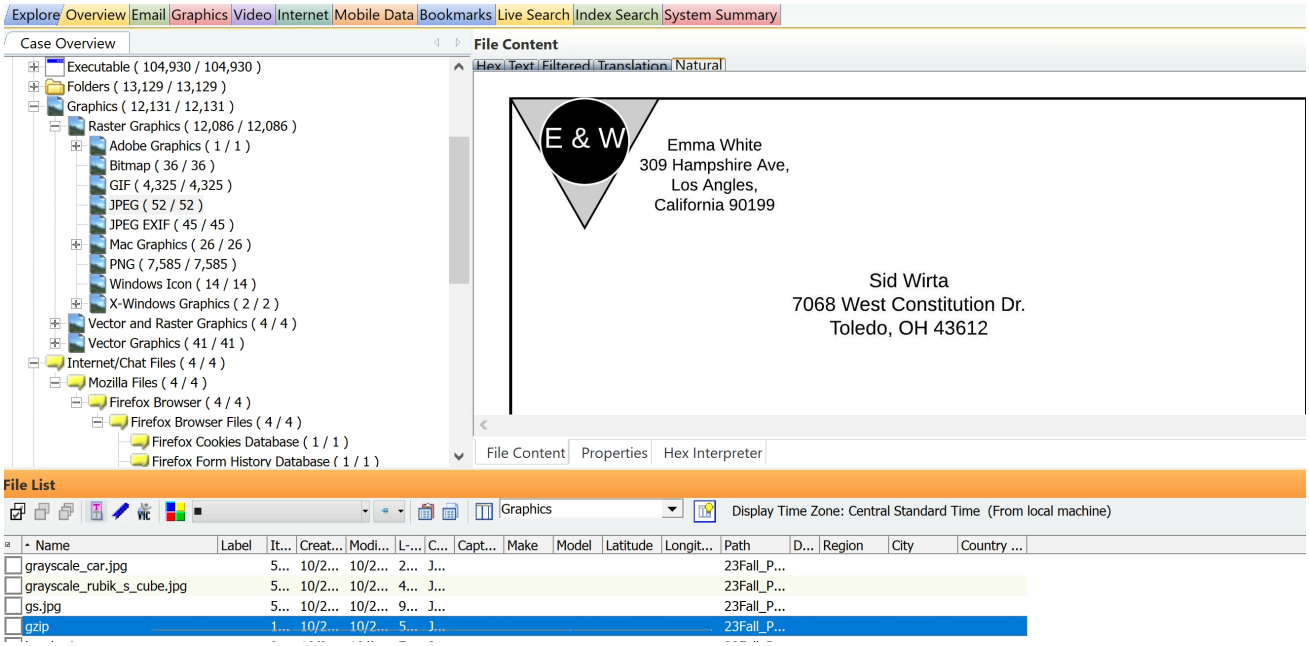
2. gzip - After not making much progress I decided to search through the File Extension tab in the Overview section while coming up with a game plan. Here I was lucky and decided to check the .gz files because there were only 6 of them. I found a compressed file named 'mypuppy.gz' with a zip file inside.



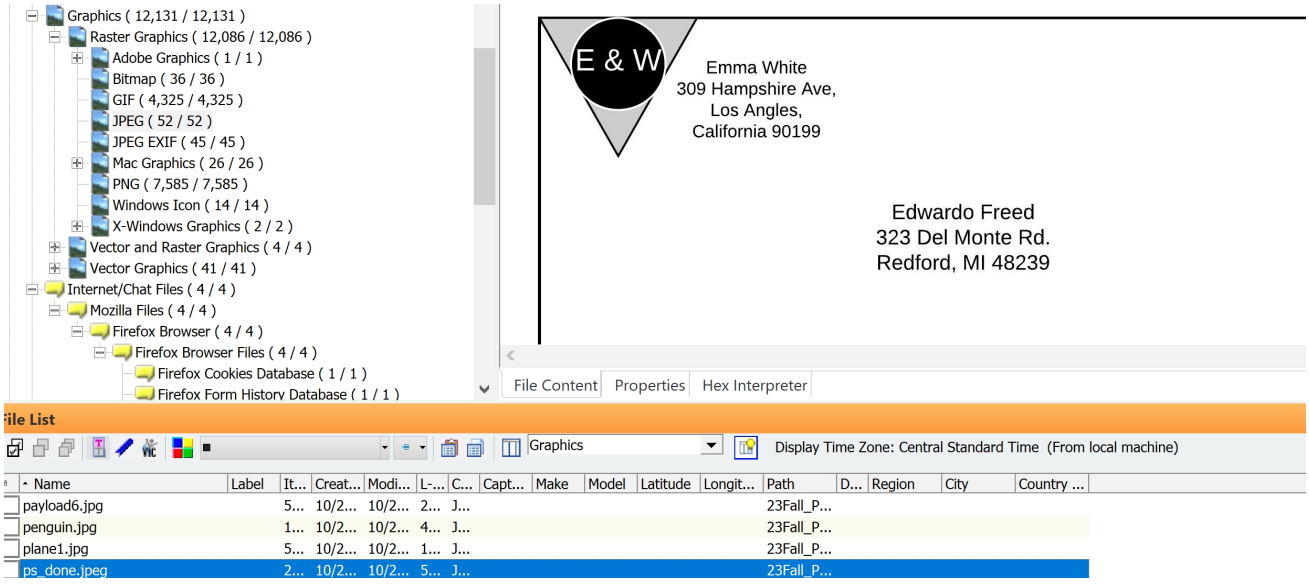
I bookmarked it and went to the index tab to see if I could find something. After using the key word 'mypuppy', i found 2 more compressed files (one zip and one 7z) and the zip file was encrypted containing a photo (more on this later).



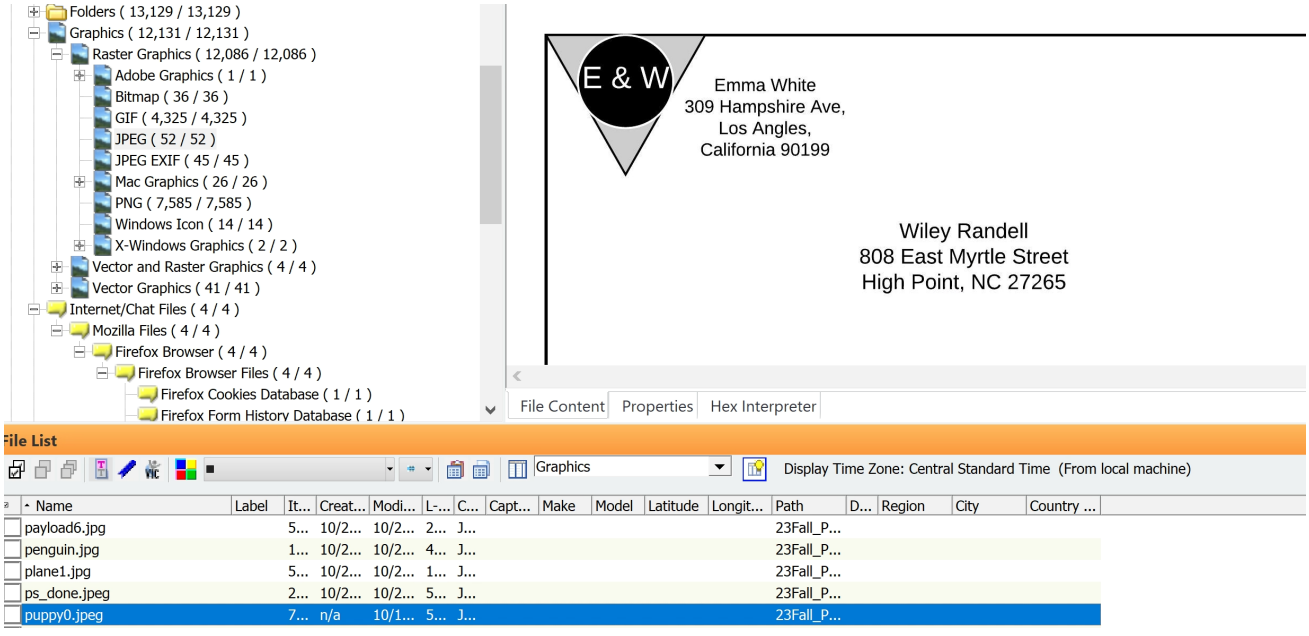
After, I searched the graphics folder for any suspicious images and found a file 'gzip' that was classified as jpeg but did not have an extension. This file contained the second envelope.



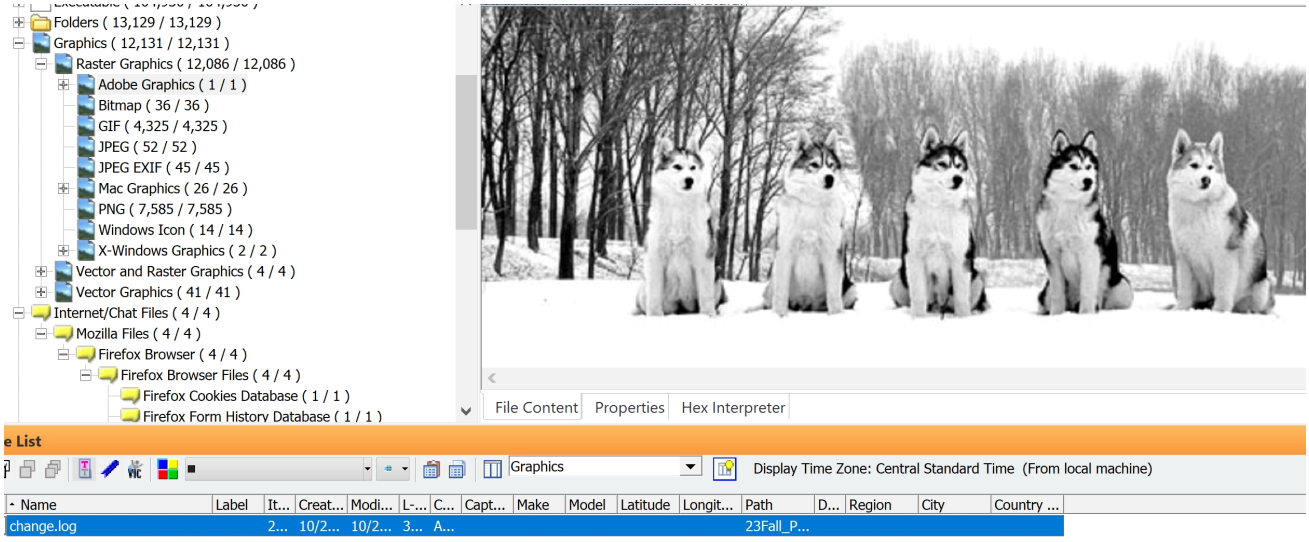
3. ps_done.jpeg - While continuing to search the graphics folder, I found two more jpeg files that contained envelopes



4. puppy0.jpeg - The second jpeg file containing an envelope talked about above.



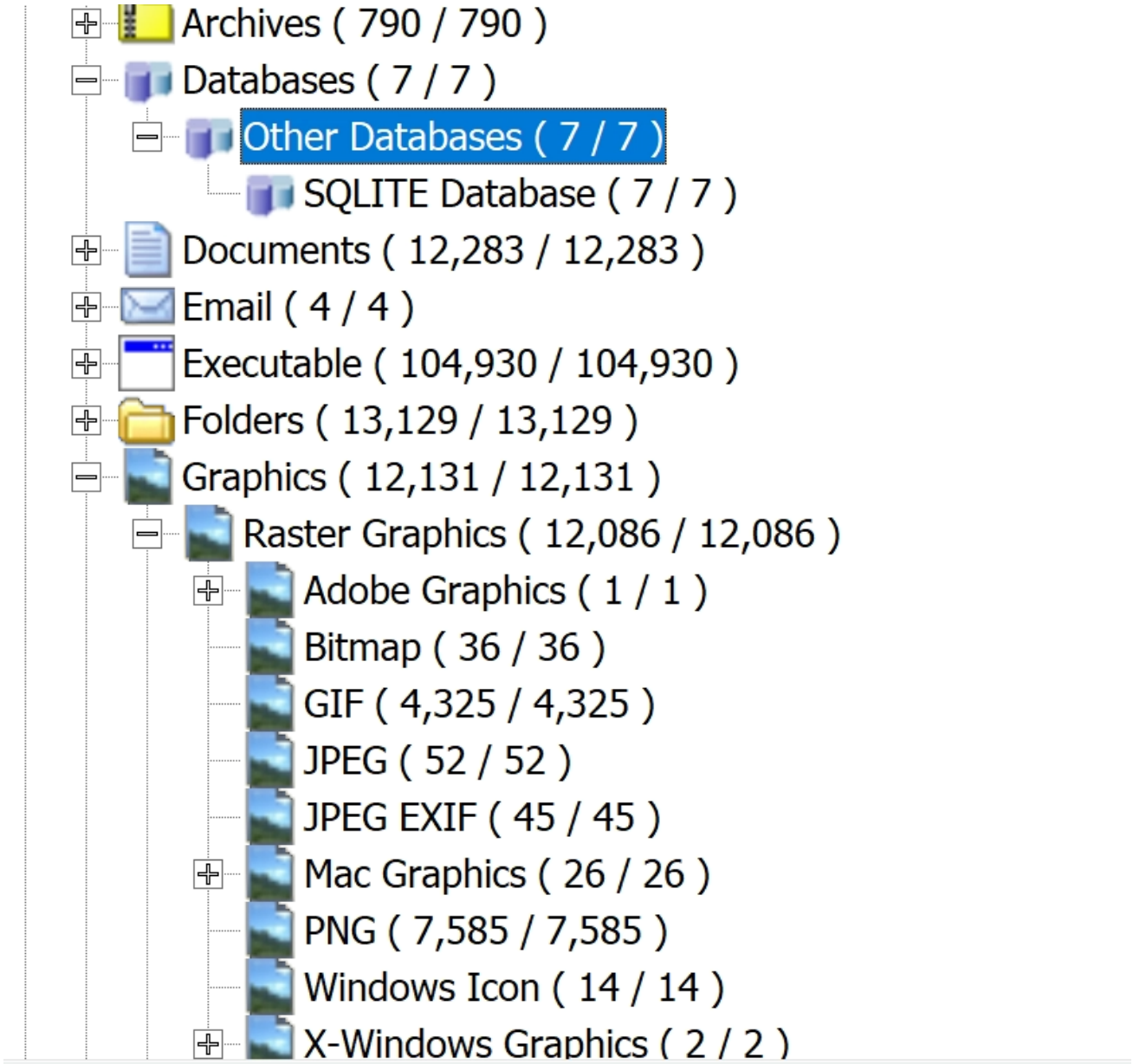
I also found many dog pictures with no information like the one below.



5. Could not find #5...

B. The suspect was found to use Firefox browser before. Please find the browsing history and list the record which website the suspect visited before.

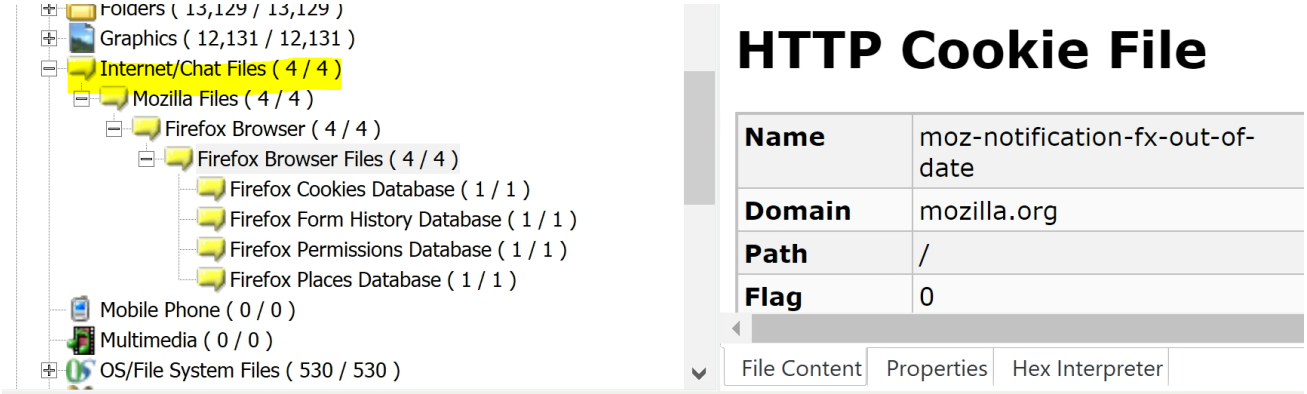
- After doing some research I found that information about the browsing history is stored in a file named 'places.sqlite' and the file 'moz_places' is the main table where you can find the URLs that have been visited. After searching the database tab in the File Categories section I only found different sqlite files.

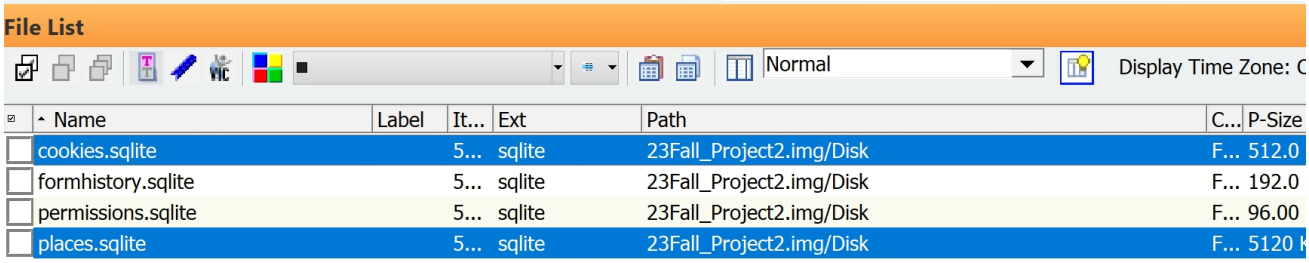


File List

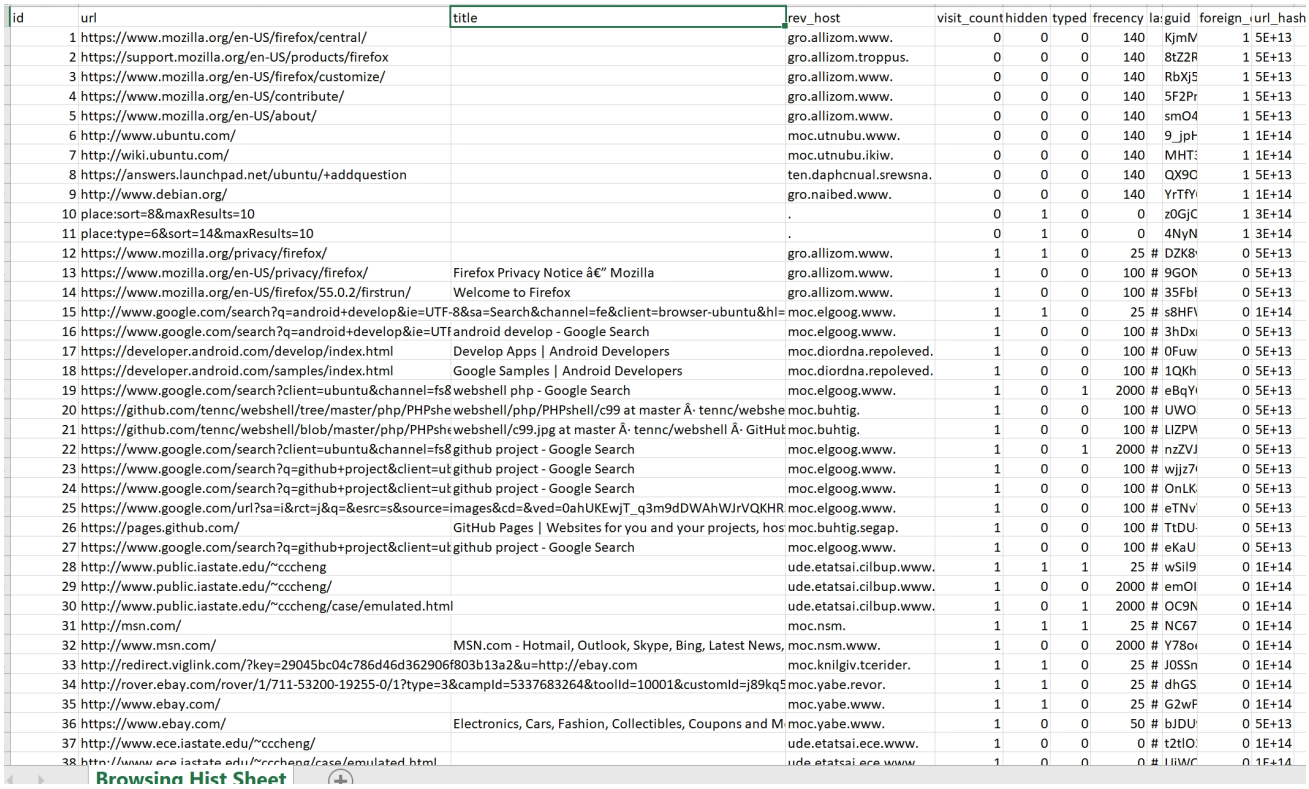
Name	Label	It...	Ext
2029012401EexhtceanCspiuotnrSa...		6...	sqlite
2918063365piupsah.sqlite		6...	sqlite
content-prefs.sqlite		5...	sqlite
favicons.sqlite		5...	sqlite
kinto.sqlite		5...	sqlite
storage.sqlite		5...	sqlite
webappsstore.sqlite		5...	sqlite

Continuing my search in the File Categories section, I found the places.sqlite file in Internet/Chat Files under Mozilla Files. Here I also found 'cookies.sqlite'.





After viewing the browser history in DBBrowser, I exported the information to a spreadsheet seen below. (38 out of 38)

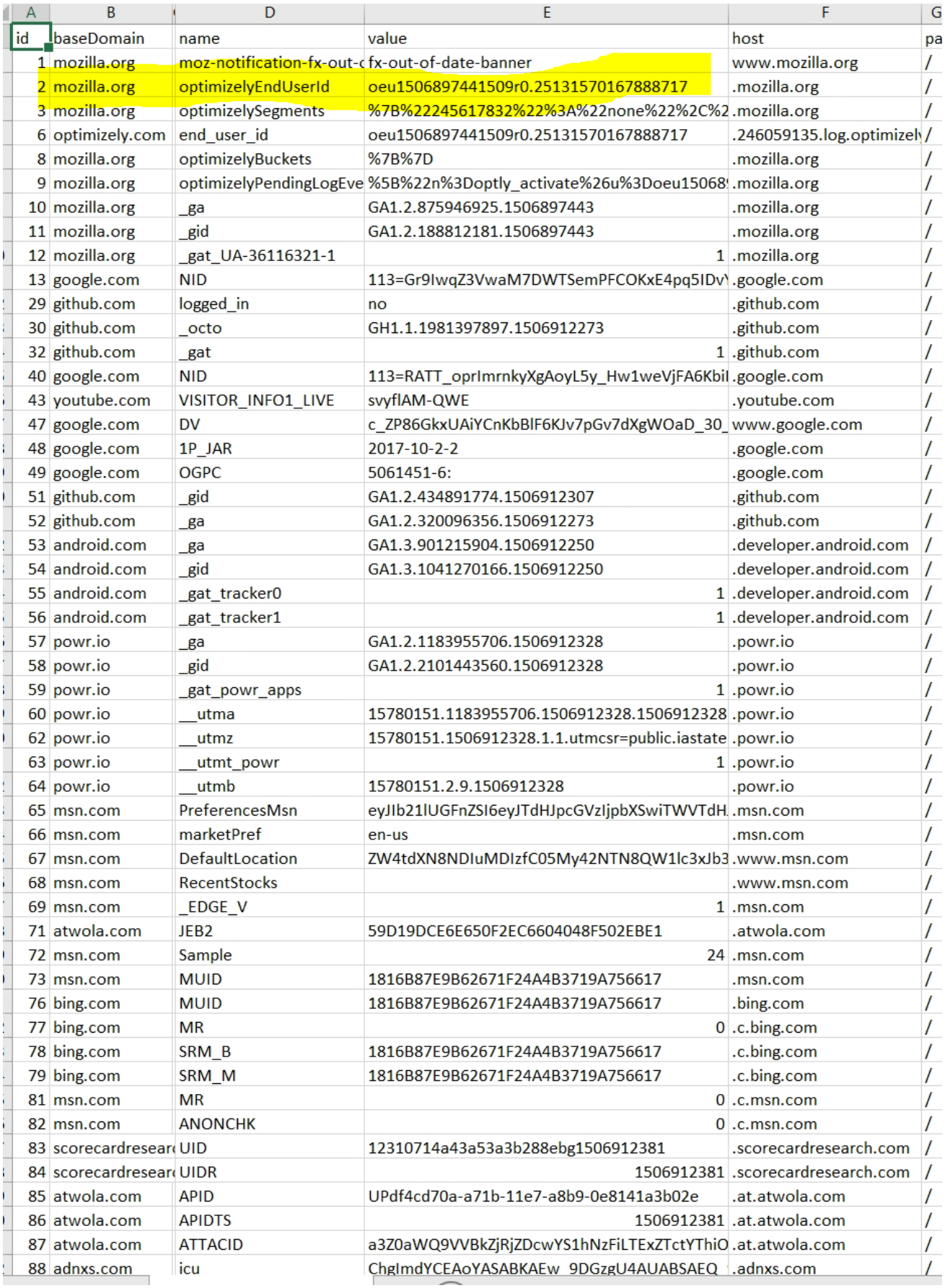


id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date	guid	foreign_count	url_hash
1	https://www.mozilla.org/en-US/firefox/central/		gro.allizom.www.	0	0	0	140		KjmM	1	5E+13
2	https://support.mozilla.org/en-US/products/firefox		gro.allizom.troppus.	0	0	0	140		8tZ2R	1	5E+13
3	https://www.mozilla.org/en-US/firefox/customize/		gro.allizom.www.	0	0	0	140		RbXj5	1	5E+13
4	https://www.mozilla.org/en-US/contribute/		gro.allizom.www.	0	0	0	140		5F2Pr	1	5E+13
5	https://www.mozilla.org/en-US/about/		gro.allizom.www.	0	0	0	140		smO4	1	5E+13
6	http://www.ubuntu.com/		moc.utnubu.www.	0	0	0	140		9_jpH	1	1E+14
7	http://wiki.ubuntu.com/		moc.utnubu.ikiw.	0	0	0	140		MHT3	1	1E+14
8	https://answers.launchpad.net/ubuntu/+addquestion		ten.daphcnual.srewsna.	0	0	0	140		QX9C	1	5E+13
9	http://www.debian.org/		gro.naibed.www.	0	0	0	140		YrTfY	1	1E+14
10	place:sort=8&maxResults=10		.	0	1	0	0		z0GjC	1	3E+14
11	place:type=6&sort=14&maxResults=10		.	0	1	0	0		4NyN	1	3E+14
12	https://www.mozilla.org/privacy/firefox/		gro.allizom.www.	1	1	0	25	#	DZK8	0	5E+13
13	https://www.mozilla.org/en-US/privacy/firefox/	Firefox Privacy Notice â€" Mozilla	gro.allizom.www.	1	0	0	100	#	9GOM	0	5E+13
14	https://www.mozilla.org/en-US/firefox/55.0.2/firstrun/	Welcome to Firefox	gro.allizom.www.	1	0	0	100	#	35FbI	0	5E+13
15	http://www.google.com/search?q=android+develop&ie=UTF-8&sa=Search&channel=fe&client=browser-ubuntu&hl=	android develop - Google Search	moc.elgoog.www.	1	1	0	25	#	s8HFV	0	1E+14
16	https://www.google.com/search?q=android+develop&ie=UTF	android develop - Google Search	moc.elgoog.www.	1	0	0	100	#	3hDx	0	5E+13
17	https://developer.android.com/develop/index.html	Develop Apps | Android Developers	moc.diordna.repoleved.	1	0	0	100	#	0Fuw	0	5E+13
18	https://developer.android.com/samples/index.html	Google Samples | Android Developers	moc.diordna.repoleved.	1	0	0	100	#	1QKh	0	5E+13
19	https://www.google.com/search?client=ubuntu&channel=fs&	webshell php - Google Search	moc.elgoog.www.	1	0	1	2000	#	eBqY	0	5E+13
20	https://github.com/tennc/webshell/tree/master/php/PHPshe	webshell/php/PHPshell/c99 at master Â· tennc/webshe	moc.buhtig.	1	0	0	100	#	UWO	0	5E+13
21	https://github.com/tennc/webshell/blob/master/php/PHPshe	webshell/c99.jpg at master Â· tennc/webshell Â· GitHut	moc.buhtig.	1	0	0	100	#	LIZPW	0	5E+13
22	https://www.google.com/search?client=ubuntu&channel=fs&	github project - Google Search	moc.elgoog.www.	1	0	1	2000	#	nzZVJ	0	5E+13
23	https://www.google.com/search?q=github+project&client=ut	github project - Google Search	moc.elgoog.www.	1	0	0	100	#	wjjz7	0	5E+13
24	https://www.google.com/search?q=github+project&client=ut	github project - Google Search	moc.elgoog.www.	1	0	0	100	#	OnLK	0	5E+13
25	https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=i	images&cd=&ved=0ahUKEwjT_q3m9dDWAhWJrVQKHR	moc.elgoog.www.	1	0	0	100	#	eTNv	0	5E+13
26	https://pages.github.com/	GitHub Pages | Websites for you and your projects, hos	moc.buhtig.segap.	1	0	0	100	#	TtDU	0	5E+13
27	https://www.google.com/search?q=github+project&client=ut	github project - Google Search	moc.elgoog.www.	1	0	0	100	#	eKaU	0	5E+13
28	http://www.public.iastate.edu/~cccheng		ude.etatsai.cilbup.www.	1	1	1	25	#	wSil9	0	1E+14
29	http://www.public.iastate.edu/~cccheng/		ude.etatsai.cilbup.www.	1	0	0	2000	#	emOI	0	1E+14
30	http://www.public.iastate.edu/~cccheng/case/emulated.html		ude.etatsai.cilbup.www.	1	0	1	2000	#	OC9N	0	1E+14
31	http://msn.com/		moc.nsm.	1	1	1	25	#	NC67	0	1E+14
32	http://www.msn.com/	MSN.com - Hotmail, Outlook, Skype, Bing, Latest News,	moc.nsm.www.	1	0	0	2000	#	Y78o	0	1E+14
33	http://redirect.viglink.com/?key=29045bc04c786d46d362906f	803b13a2&u=http://ebay.com	moc.knilgiv.tcerider.	1	1	0	25	#	J0SSn	0	1E+14
34	http://rover.ebay.com/rover/1/711-53200-19255-0/1?type=3&	campId=5337683264&toolId=10001&customId=j89kq5	moc.yabe.revor.	1	1	0	25	#	dhGS	0	1E+14
35	http://www.ebay.com/		moc.yabe.www.	1	1	0	25	#	G2wF	0	1E+14
36	https://www.ebay.com/	Electronics, Cars, Fashion, Collectibles, Coupons and M	moc.yabe.www.	1	0	0	50	#	bJDU	0	5E+13
37	http://www.ece.iastate.edu/~cccheng/		ude.etatsai.ece.www.	1	0	0	0	#	t2tlO	0	1E+14
38	http://www.ece.iastate.edu/~cccheng/case/emulated.html		ude.etatsai.ece.www.	1	0	0	0	#	UiWC	0	1E+14

Browsing Hist Sheet

C. Please list the browser cookie

- As seen above, I found this information in the cookies.sqlite file. I accessed the information through DB Browser and exported it to a excel sheet seen below. I wasn't sure if the question wanted a list of the the cookies or just the one Mozilla one. (First 52 out of 162)

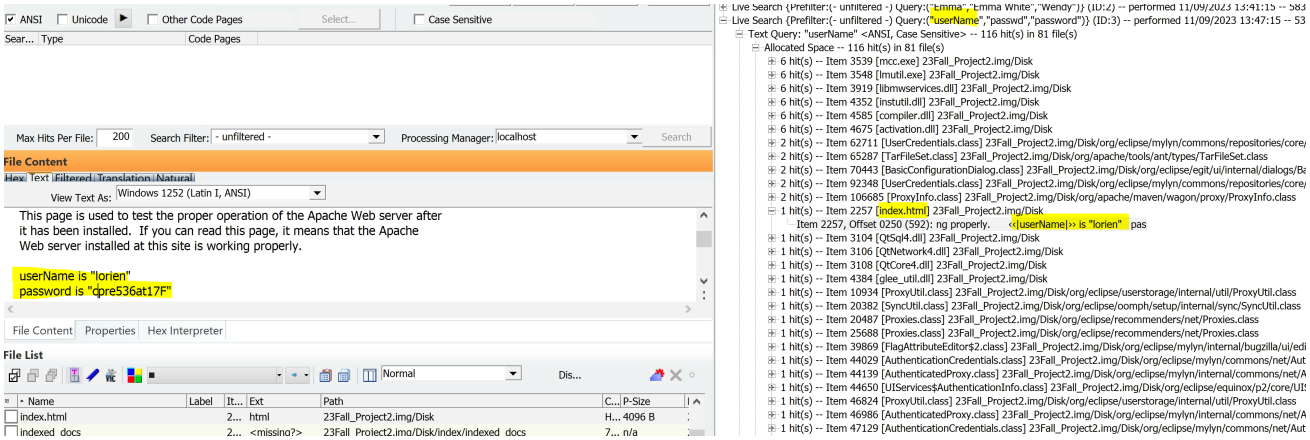


A	B	D	E	F	G
id	baseDomain	name	value	host	pa
1	mozilla.org	moz-notification-fx-out-c	fx-out-of-date-banner	www.mozilla.org	/
2	mozilla.org	optimizelyEndUserId	oeu1506897441509r0.25131570167888717	.mozilla.org	/
3	mozilla.org	optimizelySegments	%7B%22245617832%22%3A%22none%22%2C%2	.mozilla.org	/
6	optimizely.com	end_user_id	oeu1506897441509r0.25131570167888717	.246059135.log.optimizely	/
8	mozilla.org	optimizelyBuckets	%7B%7D	.mozilla.org	/
9	mozilla.org	optimizelyPendingLogEve	%5B%22n%3Doptly_activate%26u%3Doeu15068	.mozilla.org	/
10	mozilla.org	_ga	GA1.2.875946925.1506897443	.mozilla.org	/
11	mozilla.org	_gid	GA1.2.188812181.1506897443	.mozilla.org	/
12	mozilla.org	_gat_UA-36116321-1	1	.mozilla.org	/
13	google.com	NID	113=Gr9IwqZ3VwaM7DWTSemPFCOKxE4pq5IDv	.google.com	/
29	github.com	logged_in	no	.github.com	/
30	github.com	_octo	GH1.1.1981397897.1506912273	.github.com	/
32	github.com	_gat	1	.github.com	/
40	google.com	NID	113=RATT_oprImrnkyXgAoyL5y_Hw1weVjFA6KbiI	.google.com	/
43	youtube.com	VISITOR_INFO1_LIVE	svyflAM-QWE	.youtube.com	/
47	google.com	DV	c_ZP86GkxUAiYCnKbBlF6KJv7pGv7dXgWOaD_30_	www.google.com	/
48	google.com	1P_JAR	2017-10-2-2	.google.com	/
49	google.com	OGPC	5061451-6:	.google.com	/
51	github.com	_gid	GA1.2.434891774.1506912307	.github.com	/
52	github.com	_ga	GA1.2.320096356.1506912273	.github.com	/
53	android.com	_ga	GA1.3.901215904.1506912250	.developer.android.com	/
54	android.com	_gid	GA1.3.1041270166.1506912250	.developer.android.com	/
55	android.com	_gat_tracker0	1	.developer.android.com	/
56	android.com	_gat_tracker1	1	.developer.android.com	/
57	powr.io	_ga	GA1.2.1183955706.1506912328	.powr.io	/
58	powr.io	_gid	GA1.2.2101443560.1506912328	.powr.io	/
59	powr.io	_gat_powr_apps	1	.powr.io	/
60	powr.io	__utma	15780151.1183955706.1506912328.1506912328	.powr.io	/
62	powr.io	__utmz	15780151.1506912328.1.1.utmcsr=public.iastate	.powr.io	/
63	powr.io	__utmt_powr	1	.powr.io	/
64	powr.io	__utmb	15780151.2.9.1506912328	.powr.io	/
65	msn.com	PreferencesMsn	eyJlb21lUGFnZSI6eyJTdHJpcGVzIjpbXSwiTWVTdH	.msn.com	/
66	msn.com	marketPref	en-us	.msn.com	/
67	msn.com	DefaultLocation	ZW4tdXN8NDIuMDIzfC05My42NTN8QW1lc3xJb3	.www.msn.com	/
68	msn.com	RecentStocks		.www.msn.com	/
69	msn.com	_EDGE_V	1	.msn.com	/
71	atwola.com	JEB2	59D19DCE6E650F2EC6604048F502EBE1	.atwola.com	/
72	msn.com	Sample	24	.msn.com	/
73	msn.com	MUID	1816B87E9B62671F24A4B3719A756617	.msn.com	/
76	bing.com	MUID	1816B87E9B62671F24A4B3719A756617	.bing.com	/
77	bing.com	MR	0	.c.bing.com	/
78	bing.com	SRM_B	1816B87E9B62671F24A4B3719A756617	.c.bing.com	/
79	bing.com	SRM_M	1816B87E9B62671F24A4B3719A756617	.c.bing.com	/
81	msn.com	MR	0	.c.msn.com	/
82	msn.com	ANONCHK	0	.c.msn.com	/
83	scorecardresear	UID	12310714a43a53a3b288ebg1506912381	.scorecardresearch.com	/
84	scorecardresear	UIDR	1506912381	.scorecardresearch.com	/
85	atwola.com	APID	UPdf4cd70a-a71b-11e7-a8b9-0e8141a3b02e	.at.atwola.com	/
86	atwola.com	APIDTS	1506912381	.at.atwola.com	/
87	atwola.com	ATTACID	a3Z0aWQ9VVBkZjRjZDcwYS1hNzFiLTExZTctYThiO	.at.atwola.com	/
88	adnxs.com	icu	ChgImdYCEAoYASABKAEw_9DGzgU4AUABSAEQ	.adnxs.com	/

D. The suspect built a public website and there is a pair of user and password which the suspect used on website. Please find it out.

- Now that we have the browsing history, it made sense to check through there to find the public website. Unfortunately, after clicking through each link, the browsing history did not contain the public website.

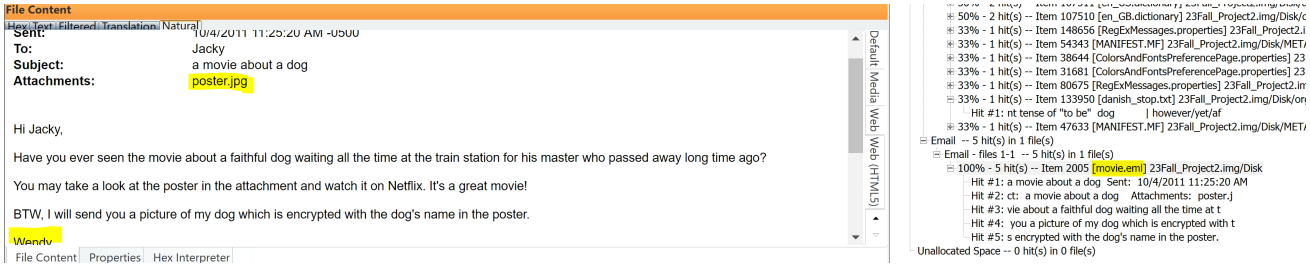
While searching for the username and password, I used the live search function to query keywords like username and password (also talked about below) and found a suspicious file when using the Test Query 'userName' with case sensitive on. The file index.html has one hit and states: 'username is "lorien"'. When i clicked on the file, I saw that right under the username line it states: 'password is "cpre536at17F"'.



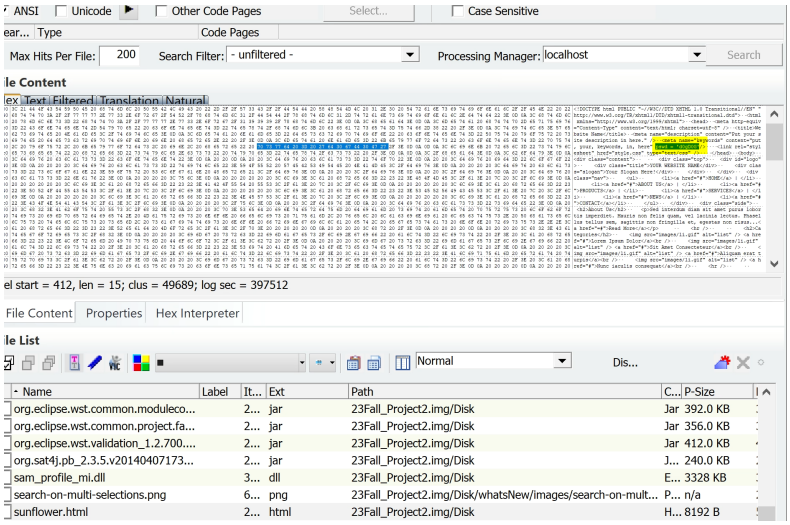
A hint given by the TA helped solidify my findings because the TA stated that the username and password would be in the same file.

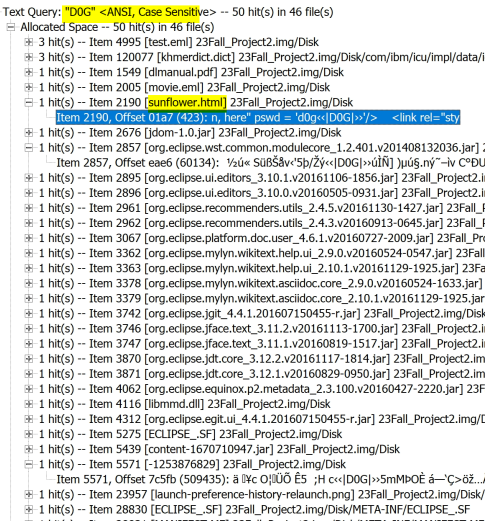
E. The suspect used a fake first name for the illegal activities, please find her real first name

- I believe Emma White was the fake name or alias and Emma's real name is Wendy as seen in the email below. With the suspicious dog photos found earlier in mind, I decided to index search for 'dog' and here I found an email file, movie.eml with five hits. Here we see information about an encrypted file as well as two new names; Jacky, the recipient, and Wendy, the sender.
- The encrypted file made me think of mypuppy.zip, the password protected zip file I found earlier.

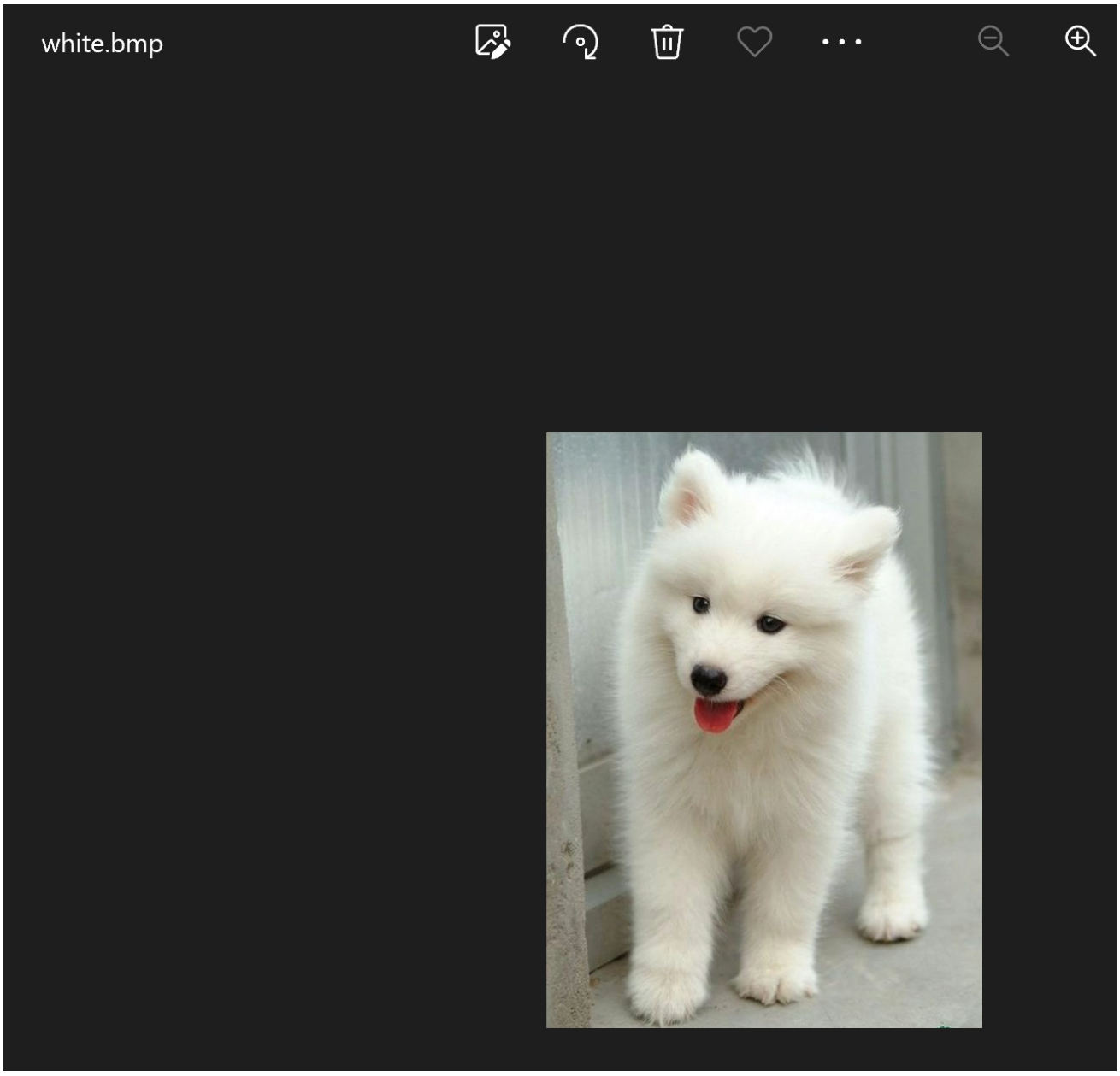


With this in mind I felt that the password and username was most likely in mypuppy.zip. I first found another zip file in the encrypted file status category called white.zip with a file called white.bmp inside. Using the live search feature, I tried a string of key words like user, secret, pswd, dog; all with various spelling types e.g. user, username; password, pass, passwd; dog, DOG, D0G, etc. The main information i found here was a possible password in the file 'sunflower.html' found with the keyword 'D0G'. The phrase states "pswd = 'd0gD0G' "





I then used this passcode to try and open the zip files and found that the code 'd0g_D0G' to unlocks the white.bmp file but not the mypuppy.jpg file. The white.bmp file seemed to be just another picture of a dog.



Lastly, i found a 'tracking.log' file that states: 'wendy-pc'. Though this is not concrete evidence, it led me to belive my pick was correct.