

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.

The screenshot shows a digital forensic interface with two main panes. The left pane is a 'Case Overview' tree view showing various file types and their counts. The right pane is a 'File Content' viewer with tabs for Hex, Text, Filtered, Translation, and Natural. A preview window shows a PDF page with an envelope containing the text: 'Emma White, 209 Hampshire Ave, Los Angeles, California 90199'. Below the preview is a 'Properties' tab. At the bottom, there's a 'File List' tab bar with icons for Explore, Overview, Email, Graphics, Video, Internet, Mobile Data, Bookmarks, Live Search, Index Search, and System Summary.

Name	Label	It...	Creat...	Modifi...	C...	L...	Ti...	Author	Last Sav...	Total...	Creat...	Last ...	P...	Revision...	Ext	D...	Path	MD5	Parent ID
UsingTeXnicCenter2.pdf		1...	10/2...	10/2...	A...	5...	M...	sloanjd			pdf	23Fall_Project2.img/Disk			4166...	1537			
transactions_art_guide.pdf		1...	10/2...	10/2...	A...	4...					pdf	23Fall_Project2.img/Disk			c0d5...	1539			
template.pdf		1...	10/2...	10/2...	A...	3...	M...				pdf	23Fall_Project2.img/Disk			f6b4...	1752			
IEEEtran_HOWTO.pdf		1...	10/2...	10/2...	A...	3...					pdf	23Fall_Project2.img/Disk			30e4...	1539			

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.

The screenshot shows a digital forensic interface with two main panes. The left pane is a 'Case Overview' tree view showing various file types and their counts. The right pane is a 'File Content' viewer with tabs for Hex, Text, Filtered, Translation, and Natural. A preview window shows the contents of a ZIP archive named 'mypuppy.zip' containing a file named 'mypuppy.jpg'. Below the preview is a 'Properties' tab. At the bottom, there's a 'File List' tab bar with icons for Explore, Overview, Email, Graphics, Video, Internet, Mobile Data, Bookmarks, Live Search, Index Search, and System Summary.

Name	Size	Modified
23Fall_Project2.img/Disk		
mypuppy.zip	388,189	10/4/2011 4:

Name	Label	It...	Ext	Path	C...	P...
mypuppy.gz		1...	gz	23Fall_Project2.img/Disk	G...	3

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).

Screenshot of a digital forensic search interface showing results for the term "mypuppy".

Search Terms:

- mypuppy (7 hits)
- dog (24 hits)
- user (7 hits)
- pass (247 hits)
- pswd (3 hits)

Results:

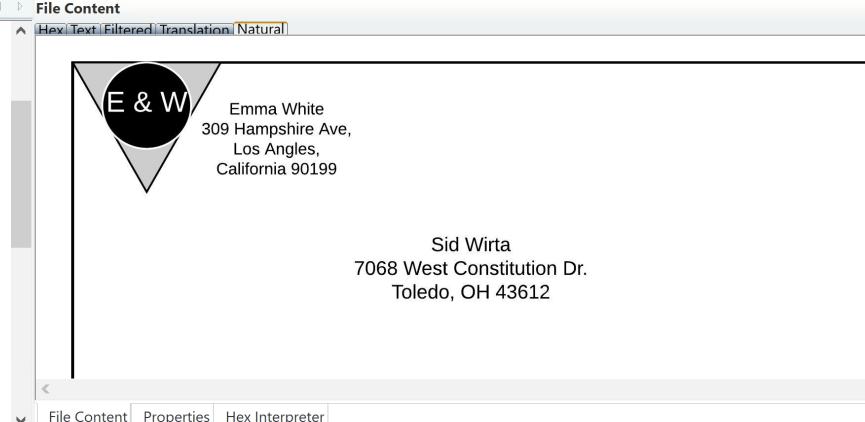
- Allocated Space -- 7 hit(s) in 5 file(s)
 - Archives -- 2 hit(s) in 2 file(s)
 - 66% - 1 hit(s) -- Item 1034 [mypuppy.zip] 23Fall_Project2.img/Disk/mypuppy.zip
 - 66% - 1 hit(s) -- Item 1536 [mypuppy.gz] 23Fall_Project2.img/Disk
 - Folders -- 1 hit(s) in 1 file(s)
 - Folders - files 1-1 -- 1 hit(s) in 1 file(s)
 - Hit #1: 71F324 mypuppy.gz mypuppy2.7z
 - Unknown Types -- 4 hit(s) in 2 file(s)
 - Unknown Types - files 1-2 -- 4 hit(s) in 2 file(s)
 - 100% - 2 hit(s) -- Item 76147 [mypuppy.jpg] 23Fall_Project2.img/Disk/mypuppy.zip/mypuppy.jpg
 - 100% - 2 hit(s) -- Item 1013 [SMFT] 23Fall_Project2.img/Disk
- Unallocated Space -- 0 hit(s) in 0 file(s)

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.

Screenshot of a digital forensic interface showing the Case Overview and File Content tabs.

Case Overview:

- Executable (104,930 / 104,930)
- Folders (13,129 / 13,129)
- Graphics (12,131 / 12,131)
 - Raster Graphics (12,086 / 12,086)
 - Adobe Graphics (1 / 1)
 - Bitmap (36 / 36)
 - GIF (4,325 / 4,325)
 - JPEG (52 / 52)
 - JPEG EXIF (45 / 45)
 - Mac Graphics (26 / 26)
 - PNG (7,585 / 7,585)
 - Windows Icon (14 / 14)
 - X-Windows Graphics (2 / 2)
 - Vector and Raster Graphics (4 / 4)
 - Vector Graphics (41 / 41)
- Internet/Chat Files (4 / 4)
 - Mozilla Files (4 / 4)
 - Firefox Browser (4 / 4)
 - Firefox Browser Files (4 / 4)
 - Firefox Cookies Database (1 / 1)
 - Firefox Form History Database (1 / 1)



File List:

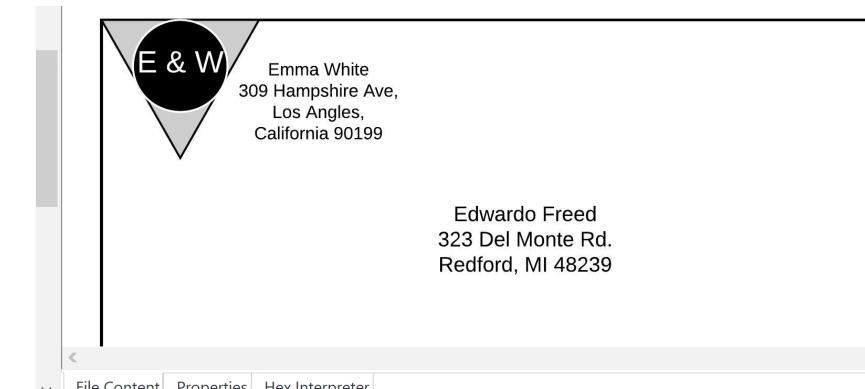
Name	Label	It...	Creat...	Modi...	L...	C...	Capt...	Make	Model	Latitude	Longit...	Path	D...	Region	City	Country ...
grayscale_car.jpg		5...	10/2...	10/2...	2...	J...							23Fall_P...			
grayscale_rubik_s_cube.jpg		5...	10/2...	10/2...	4...	J...							23Fall_P...			
gs.jpg		5...	10/2...	10/2...	9...	J...							23Fall_P...			
gzip		1...	10/2...	10/2...	5...	J...							23Fall_P...			

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

Screenshot of a digital forensic interface showing the Case Overview and File Content tabs.

Case Overview:

- Graphics (12,131 / 12,131)
 - Raster Graphics (12,086 / 12,086)
 - Adobe Graphics (1 / 1)
 - Bitmap (36 / 36)
 - GIF (4,325 / 4,325)
 - JPEG (52 / 52)
 - JPEG EXIF (45 / 45)
 - Mac Graphics (26 / 26)
 - PNG (7,585 / 7,585)
 - Windows Icon (14 / 14)
 - X-Windows Graphics (2 / 2)
 - Vector and Raster Graphics (4 / 4)
 - Vector Graphics (41 / 41)
- Internet/Chat Files (4 / 4)
 - Mozilla Files (4 / 4)
 - Firefox Browser (4 / 4)
 - Firefox Browser Files (4 / 4)
 - Firefox Cookies Database (1 / 1)
 - Firefox Form History Database (1 / 1)



File List:

Name	Label	It...	Creat...	Modi...	L...	C...	Capt...	Make	Model	Latitude	Longit...	Path	D...	Region	City	Country ...
payload6.jpg		5...	10/2...	10/2...	2...	J...							23Fall_P...			
penguin.jpg		1...	10/2...	10/2...	4...	J...							23Fall_P...			
plane1.jpg		5...	10/2...	10/2...	1...	J...							23Fall_P...			
ps_done.jpeg		2...	10/2...	10/2...	5...	J...							23Fall_P...			

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

The screenshot shows a file explorer interface with a tree view on the left and a list view on the right. The tree view shows a hierarchy of folders and files under 'Graphics'. The list view shows several files, with 'puppy0.jpeg' highlighted in blue. Below the list view is a preview window showing a black and white image of an envelope with 'E & W' on it.

Name	Label	It...	Creat...	Modi...	L...	C...	Capt...	Make	Model	Latitude	Longit...	Path	D...	Region	City	Country ...
payload6.jpg		5...	10/2...	10/2...	2...	J...						23Fall_P...				
penguin.jpg		1...	10/2...	10/2...	4...	J...						23Fall_P...				
plane1.jpg		5...	10/2...	10/2...	1...	J...						23Fall_P...				
ps_done.jpeg		2...	10/2...	10/2...	5...	J...						23Fall_P...				
puppy0.jpeg		7...	n/a	10/1...	5...	J...						23Fall_P...				

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

The screenshot shows a file explorer interface with a tree view on the left and a preview window on the right. The tree view shows a hierarchy of folders and files under 'Graphics'. The preview window shows a large image of four husky dogs sitting in a snowy forest. Below the preview window is a list view showing a single file named 'change.log'.

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 Tree:

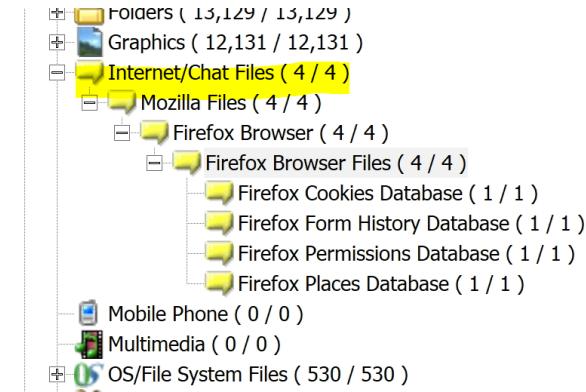
- + Archives (790 / 790)
- Databases (7 / 7)
 - Other Databases (7 / 7)
 - SQLITE Database (7 / 7)
- + Documents (12,283 / 12,283)
- + Email (4 / 4)
- + Executable (104,930 / 104,930)
- + Folders (13,129 / 13,129)
- Graphics (12,131 / 12,131)
 - Raster Graphics (12,086 / 12,086)
 - + Adobe Graphics (1 / 1)
 - + Bitmap (36 / 36)
 - + GIF (4,325 / 4,325)
 - + JPEG (52 / 52)
 - + JPEG EXIF (45 / 45)
 - + Mac Graphics (26 / 26)
 - + PNG (7,585 / 7,585)
 - + Windows Icon (14 / 14)
 - + X-Windows Graphics (2 / 2)

File List



	Name	Label	It...	Ext
<input type="checkbox"/>	2029012401EexhtceanCspiuotnrSa...	6...		sqlite
<input type="checkbox"/>	2918063365piupsah.sqlite	6...		sqlite
<input type="checkbox"/>	content-prefs.sqlite	5...		sqlite
<input type="checkbox"/>	favicons.sqlite	5...		sqlite
<input type="checkbox"/>	kinto.sqlite	5...		sqlite
<input type="checkbox"/>	storage.sqlite	5...		sqlite
<input type="checkbox"/>	webappsstore.salite	5...		salite

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'.



HTTP Cookie File

Name	moz-notification-fx-out-of-date
Domain	mozilla.org
Path	/
Flag	0

File Content Properties Hex Interpreter

File List					
	Name	Label	It...	Ext	Path
	cookies.sqlite	5...	sqlite	.sqlite	23Fall_Project2.img/Disk
	formhistory.sqlite	5...	sqlite	.sqlite	23Fall_Project2.img/Disk
	permissions.sqlite	5...	sqlite	.sqlite	23Fall_Project2.img/Disk
	places.sqlite	5...	sqlite	.sqlite	23Fall_Project2.img/Disk

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	La_Guid	Foreign_Url_Hash
1	https://www.mozilla.org/en-US/firefox/central/		gro.allizom.www.	0	0	0	140	KjmIV	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.ubuntu.www.	0	0	0	140	9_jpF	1.1E+14
7	http://wiki.ubuntu.com/		moc.ubuntu.ikiw.	0	0	0	140	MHT:	1.1E+14
8	https://answers.launchpad.net/ubuntu/+addquestion		ten.daphnual.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	zOGJC	1.3E+14
11	place:type=6&sort=14&maxResults=10		.	0	1	0	0	4NynY	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 # 9GON	0	5E+13
14	https://www.mozilla.org/en-US/firefox/55.0.2/fire/run/	Welcome to Firefox	gro.allizom.www.	1	0	0	100 # 35fbL	0	5E+13
15	https://www.google.com/search?q=android+develop&ie=UTF-8&sas=Search&channel=fe&client=firefox-ubuntu&hl=		moc.elgoog.www.	1	1	0	25 # s8HFV	0	1E+14
16	https://www.google.com/search?q=android+develop&ie=UTF8&channel=fe&client=firefox-ubuntu&hl=		moc.elgoog.www.	1	0	0	100 # 3hDxi	0	5E+13
17	https://developer.android.com/develop/index.html	Develop Apps Android Developers	moc.diordna.repoledev.	1	0	0	100 # 0Fuw	0	5E+13
18	https://developer.android.com/samples/index.html	Google Samples Android Developers	moc.diordna.repoledev.	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 # ebqYI	0	5E+13
20	https://github.com/tennc/webshell/tree/master/php/PHPshe/webshell/php/PHPshe/c99 at master Â· tennnc/webshe/moc.buhtig.		1	0	0	100 # UW0	0	5E+13	
21	https://github.com/tennc/webshell/blob/master/php/PHPshe/webshell/c99.jpg at master Â· tennnc/webshell Â· GitHut/moc.buhtig.		1	0	0	100 # LIZPM	0	5E+13	
22	https://www.google.com/search?client=ubuntu&channel=fs&github project - Google Search		moc.elgoog.www.	1	0	1	2000 # nzVJl	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=images&rcd=&ved=0ahUKEwjT_q3m9dDWAhWlVQKHz.moc.elgoog.www.		1	0	0	100 # eTNv	0	5E+13	
26	https://pages.github.com/	GitHub Pages Websites for you and your projects, hosted by GitHub	moc.elgoog.www.	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 # wSiI9	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 # Y78oI	0	1E+14	
33	http://redirect.viglink.com/?key=29045bc04c786d46d362906f803b13a2&u=http://ebay.com		moc.knlivg.tcriderv.	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=j89kq5moc.yabe.revor.		1	1	0	25 # dhIGS	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 More 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 # t2tIO	0	1E+14
38	http://www.ece.iastate.edu/~cccheng/case/emulated.html		ude.etatsai.ece.www.	1	0	0	0 # liiWC	0	1E+14

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-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.optimizel	/
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=Gr9lwqZ3VwaM7DWTSemPFCOKxE4pq5IDv	.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_oprlmrnkyXgAoyL5y_Hw1weVjFA6Kbil	.google.com	/
43	youtube.com	VISITOR_INFO1_LIVE	svyflAM-QWE	.youtube.com	/
47	google.com	DV	c_ZP86GkxUAiYCnKbBf6KJv7pGv7dXgWOaD_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.utmcsrc=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	eyJlb21lUGFnZSI6eyJTdHJpcGVzIpbXSwiTWWTdH	.msn.com	/
66	msn.com	marketPref	en-us	.msn.com	/
67	msn.com	DefaultLocation	ZW4tdXN8NDluMDIzfC05My42NTN8QW1lc3xJb3	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	scorecardresearch.com	UID	12310714a43a53a3b288ebg1506912381	.scorecardresearch.com	/
84	scorecardresearch.com	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	adnx.com	icu	ChglmdYCEAoYASABKAEw_9DGzgU4AUABSAEQ	.adnx.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"'.

The screenshot shows the NetworkMiner interface with a live search results pane on the right. The search term is 'userName' with the 'Case Sensitive' option checked. The results list contains numerous hits across various files and protocols, with the top hit being 'index.html' at offset 250 (592). The content of 'index.html' is displayed in the main pane, showing the text 'username is "lorien"' and '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.

The screenshot shows an email message from 'Wendy' to 'Jacky'. The subject is 'a movie about a dog' and the attachment is 'poster.jpg'. The message body starts with 'Hi Jacky,' and continues with 'Have you ever seen the movie about a faithful dog waiting all the time at the train station for his master who passed away long time ago? You may take a look at the poster in the attachment and watch it on Netflix. It's a great movie! BTW, I will send you a picture of my dog which is encrypted with the dog's name in the poster.'

```

Live Search {Prefilter:(- unfiltered -) Query:(["Emma", "Emma White", "Wendy"]) (IU:Z) -- performed 11/09/2023 13:41:15 -- 588
Live Search {Prefilter:(- unfiltered -) Query:(["userName", "password", "password"]) (ID:3) -- performed 11/09/2023 13:47:15 -- 53
Text Query: "userName" <ANSI, Case Sensitive> -- 116 hit(s) in 81 file(s)
  Allocated Space -- 116 hit(s) in 81 file(s)
  + 6 hit(s) -- Item 3539 [Inno.exe] 23Fall_Project2.img/Disk
  + 6 hit(s) -- Item 3548 [Imutil.exe] 23Fall_Project2.img/Disk
  + 6 hit(s) -- Item 3919 [libcurl.dll] 23Fall_Project2.img/Disk
  + 6 hit(s) -- Item 4001 [curl.dll] 23Fall_Project2.img/Disk
  + 6 hit(s) -- Item 4505 [Compiler.dll] 23Fall_Project2.img/Disk
  + 2 hit(s) -- Item 62711 [UserCredentials.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/commons/repositories/core/
  + 2 hit(s) -- Item 65287 [TarFileSet.class] 23Fall_Project2.img/Disk/org/apache/tools/art/types/TarFileSet.class
  + 2 hit(s) -- Item 70443 [BasicConfigurationDialog.class] 23Fall_Project2.img/Disk/org/eclipse/egit/ui/internal/dialogs/B
  + 2 hit(s) -- Item 92348 [UserCredentials.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/commons/repositories/core/
  + 2 hit(s) -- Item 106685 [ProxyInfo.class] 23Fall_Project2.img/Disk/org/apache/maven/wagon/proxy/ProxyInfo.class
  + 1 hit(s) -- Item 2257 [Index.html] 23Fall_Project2.img/Disk
    Item 2257, Offset 0250 (592): ng properly. <UserName> is "lorien" pas
  + 1 hit(s) -- Item 3104 [QtSql.dll] 23Fall_Project2.img/Disk
  + 1 hit(s) -- Item 3106 [QtNetwork.dll] 23Fall_Project2.img/Disk
  + 1 hit(s) -- Item 3108 [QtCore4.dll] 23Fall_Project2.img/Disk
  + 1 hit(s) -- Item 4384 [glew_util.dll] 23Fall_Project2.img/Disk
  + 1 hit(s) -- Item 10934 [ProxyUtil.class] 23Fall_Project2.img/Disk/org/eclipse/userstorage/internal/Util/ProxyUtil.class
  + 1 hit(s) -- Item 20382 [SyncUtil.class] 23Fall_Project2.img/Disk/org/eclipse/oomph/setup/internal/sync/SyncUtil.class
  + 1 hit(s) -- Item 20487 [Proxies.class] 23Fall_Project2.img/Disk/org/eclipse/recommenders/net/Proxies.class
  + 1 hit(s) -- Item 25688 [Proxies.class] 23Fall_Project2.img/Disk/org/eclipse/recommenders/net/Proxies.class
  + 1 hit(s) -- Item 39869 [FlagAttributeEditor$2.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/internal/bugzilla/ui/edi
  + 1 hit(s) -- Item 44029 [AuthenticationCredentials.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/commons/net/Aut
  + 1 hit(s) -- Item 44139 [AuthenticatedProxy.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/internal/commons/net/A
  + 1 hit(s) -- Item 44650 [UIServicesAuthenticationInfo.class] 23Fall_Project2.img/Disk/org/eclipse/equinix/p2/core/U
  + 1 hit(s) -- Item 46824 [ProxyUtil.class] 23Fall_Project2.img/Disk/org/eclipse/userstorage/internal/Util/ProxyUtil.class
  + 1 hit(s) -- Item 46986 [AuthenticatedProxy.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/internal/commons/net/A
  + 1 hit(s) -- Item 47129 [AuthenticationCredentials.class] 23Fall_Project2.img/Disk/org/eclipse/mylyn/commons/net/Aut

```

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'"

S ANSI Unicode Case Sensitive

File Content Properties Hex Interpreter

le List

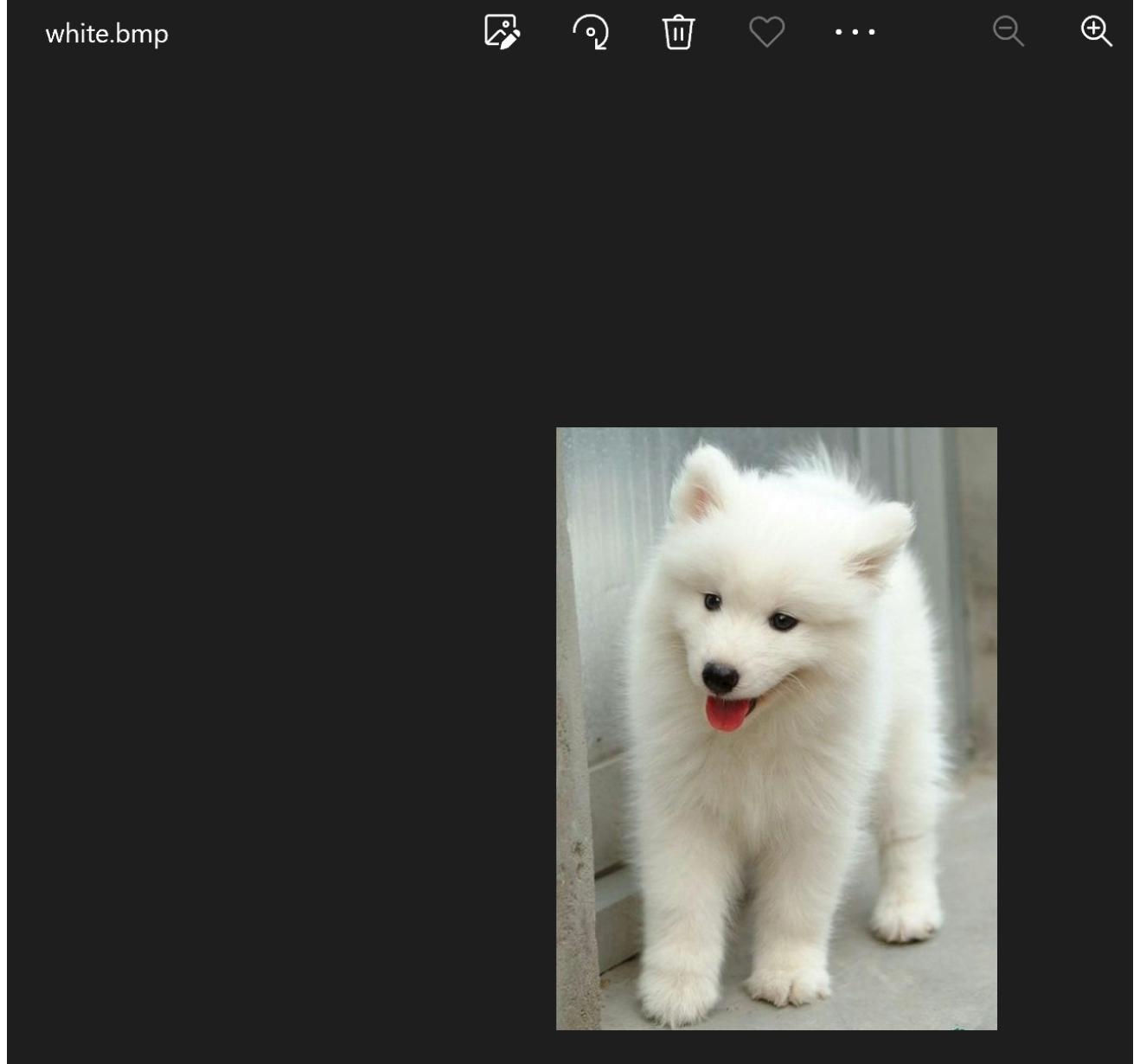
Name	Label	IT...	Ext	Path	C...	P-Size	I
org.eclipse.wst.common.modulco...		2...	Jar	23Fall_Project2Disk	Jar	392.0 KB	.
org.eclipse.wst.common.projectfa...		2...	Jar	23Fall_Project2Disk	Jar	356.0 KB	.
org.eclipse.wst.validation_1.2.700...		2...	Jar	23Fall_Project2Disk	Jar	412.0 KB	.
org.sat4j.pb_3.5.5.v20140717...		2...	Jar	23Fall_Project2Disk	Jar	240.0 KB	.
sam_profile_mi.dll		3...	dll	23Fall_Project2Disk	E...	3328 KB	.
search-on-multi-selections.png		6...	png	23Fall_Project2Disk/whatsNew/Images/search-on-mult...	P...	n/a	.
sunflower.html		2...	html	23Fall_Project2Disk	H...	8192 B	.

Text Query: "D0G" <ANSI, Case Sensitive> -- 50 hit(s) in 46 file(s)

Allocated Space -- 50 hit(s) in 46 file(s)

- * 3 hit(s) -- Item 4995 [test.eml] 23Fall_Project2Disk
- * 3 hit(s) -- Item 120077 [khmerdict.dict] 23Fall_Project2Disk/Disk/com.ibm/icu/impl/data/i
- * 1 hit(s) -- Item 1549 [dmanual.pdf] 23Fall_Project2Disk
- * 1 hit(s) -- Item 2005 [moven.eml] 23Fall_Project2Disk
- * 1 hit(s) -- Item 2190 [sunflower.html] 23Fall_Project2Disk
- [Item 2190, Offset 01a? (423): n, here pswd = d0g<|D0G|>/> - link rel="sty
- * 1 hit(s) -- Item 2676 [jdom-1.0.jar] 23Fall_Project2Disk
- 1 hit(s) -- Item 2857 [org.eclipse.wst.common.modulco..._1.2.401.v201408132036.jar] : Item 2857, Offset ea6 (60134): YB3v^5p/Zy<|D0G|>=JN! juB7ny" -> C'DU
- * 1 hit(s) -- Item 2895 [org.eclipse.ui.editors_3.10.0.v20161105-1856.jar] 23Fall_Project2.i
- * 1 hit(s) -- Item 2962 [org.eclipse.jface.text_3.10.0.v20160505-0931.jar] 23Fall_Project2.i
- * 1 hit(s) -- Item 2961 [org.eclipse.recommenders.util_2.4.5.v20161130-1427.jar] 23Fall_i
- * 1 hit(s) -- Item 3067 [org.eclipse.platform.doc.user_4.6.1.v20160727-2009.jar] 23Fall_P
- * 1 hit(s) -- Item 3362 [org.eclipse.mylyn.wikitext.help.ui_2.9.0.v20160524-0547.jar] 23Fall
- * 1 hit(s) -- Item 3363 [org.eclipse.mylyn.wikitext.help.ui_2.10.1.v20161129-1925.jar] 23Fa
- * 1 hit(s) -- Item 3378 [org.eclipse.mylyn.wikitext.asciidoc.core_2.9.0.v20160524-1633.jar] : Item 3378, Offset ee4 (61216): 9!C0!VW10!fJt!9R!<|D0G|>=JN! juB7ny" -> C'DU
- * 1 hit(s) -- Item 3379 [org.eclipse.mylyn.wikitext.asciidoc.core_2.10.1.v20161129-1925.jar] : Item 3379, Offset 01a? (423): n, here pswd = d0g<|D0G|>/> - link rel="sty
- 1 hit(s) -- Item 3742 [org.eclipse.jgit_4.4.1.201607150455-r.jar] 23Fall_Project2Disk
- * 1 hit(s) -- Item 5439 [content-1670710947.jar] 23Fall_Project2Disk
- * 1 hit(s) -- Item 5571 [content-1670710947.jar] 23Fall_Project2Disk
- [Item 5571, Offset 7c5fb (509435): àÍÓ!JÚÖ ÈS ,H<<|D0G|>>5mMP0É á—>C@öž..]
- * 1 hit(s) -- Item 23957 [launch-preference-history-relaunch.png] 23Fall_Project2Disk/
- * 1 hit(s) -- Item 28830 [ECLIPSE_SF] 23Fall_Project2Disk/META-INF/ECLIPSE_SF

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.