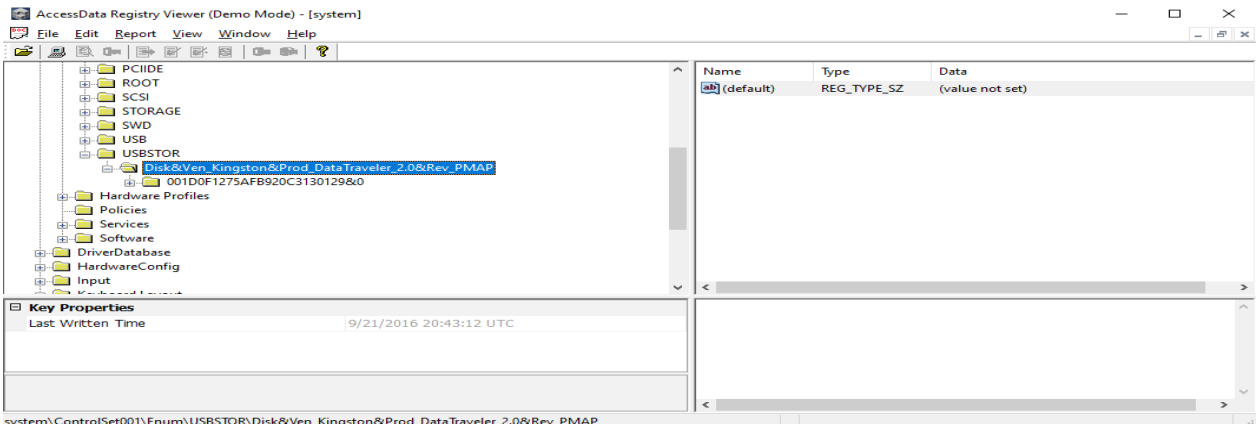
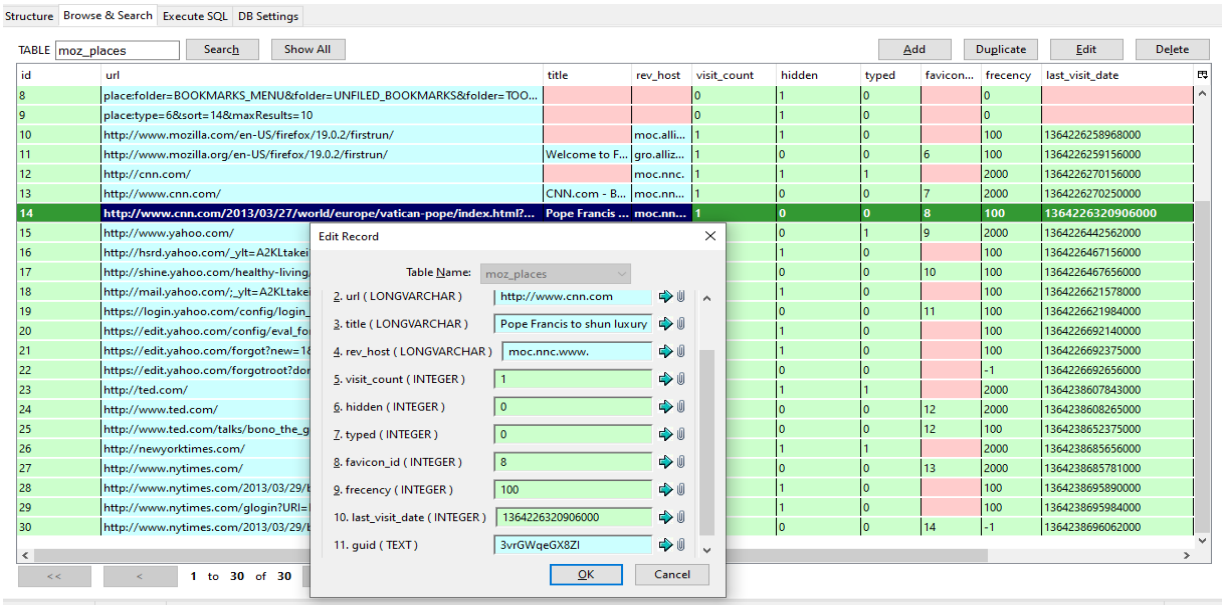
Laboratory Notes

Laboratory Number: 3 Examiner Name: Akshay Chaurasia

Date & Time	Activity
10/12/19 3:00 PM	1. When you find the correct key, **take a screenshot of the key** to include in forensic notes 
10/12/19 3:25 PM	2. Browse through the SQL table a. What is the URL of the website that the user viewed concerning Pope Francis?
3:30 PM	http://www.cnn.com/2013/03/27/world/europe/vatican-pope/index.html?hpt=hp_bn2 
3:35 PM	b. What was the date and time the site was visited? Integer Date: 1364226320906000

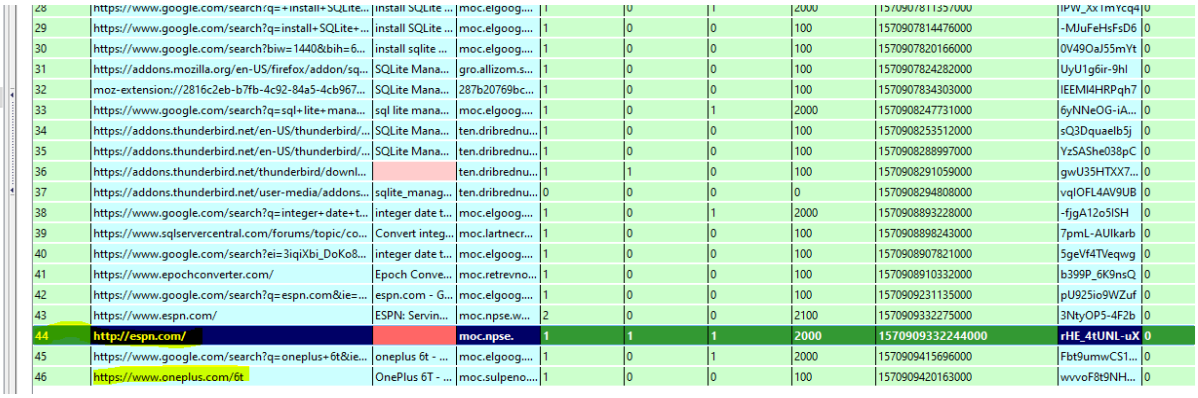
Assuming that this timestamp is in **microseconds (1/1,000,000 second)**:
GMT: Monday, March 25, 2013 3:45:20.906 PM
Your time zone: Monday, March 25, 2013 11:45:20.906 AM GMT-04:00 DST
Relative: 7 years ago

3. Which website was recorded into the browser's history?

I visited two websites in the normal browsing mode- https://www.oneplus.com/6t and http://espn.com/
Both the websites were recorded.

But the websites that I visited in private mode using the firefox web browser were not recorded.

3:40 PM



29	https://www.google.com/search?q=install+SQLite+...	install SQLite ...	moc.elgoog....	1	0	0	100	1570907814476000	-MJuFeHsFsD6	0
30	https://www.google.com/search?biw=1440&bih=6...	install sqlite ...	moc.elgoog....	1	0	0	100	1570907820166000	0V49OaJ55mYt	0
31	https://addons.mozilla.org/en-US/firefox/addon/sq...	SQLite Mana...	gro.allizom.s...	1	0	0	100	1570907824282000	UyU1g6ir-9hI	0
32	moz-extension://2816c2eb-b7fb-4c92-84a5-4cb967...	SQLite Mana...	287b20769bc...	1	0	0	100	1570907834303000	IEEMI4HRPqh7	0
33	https://www.google.com/search?q=sql+lite+mana...	sql lite mana...	moc.elgoog....	1	0	1	2000	1570908247731000	6yNNeOG-iA...	0
34	https://addons.thunderbird.net/en-US/thunderbird/...	SQLite Mana...	ten.dribrednu...	1	0	0	100	1570908253512000	sQ3Dquaelb5j	0
35	https://addons.thunderbird.net/en-US/thunderbird/...	SQLite Mana...	ten.dribrednu...	1	0	0	100	1570908288997000	YzSAShe038pC	0
36	https://addons.thunderbird.net/thunderbird/downl...		ten.dribrednu...	1	1	0	100	1570908291059000	gwU35HTXX7...	0
37	https://addons.thunderbird.net/user-media/addons...	sqlite_manag...	ten.dribrednu...	0	0	0	0	1570908294808000	vqlOFL4AV9UB	0
38	https://www.google.com/search?q=integer+date+t...	integer date t...	moc.elgoog....	1	0	1	2000	1570908893228000	-fjgA12o5lSH	0
39	https://www.sqlservercentral.com/forums/topic/co...	Convert integ...	moc.lartnecr...	1	0	0	100	1570908898243000	7pmL-AUlkarb	0
40	https://www.google.com/search?ei=3iqiXbi_DoKo8...	integer date t...	moc.elgoog....	1	0	0	100	1570908907821000	5geVf4TVeqwg	0
41	https://www.epochconverter.com/	Epoch Conve...	moc.retrevno...	1	0	0	100	1570908910332000	b399P_6K9nsQ	0
42	https://www.google.com/search?q=espn.com&ie=...	espn.com - G...	moc.elgoog....	1	0	0	100	1570909231135000	pU925io9WZuf	0
43	https://www.espn.com/	ESPN: Servin...	moc.npse.w...	2	0	0	2100	1570909332275000	3NtyOP5-4F2b	0
44	http://espn.com/		moc.npse.	1	1	1	2000	1570909332244000	rHE_4tUNL-uX	0
45	https://www.google.com/search?q=oneplus+6t&ie...	oneplus 6t - ...	moc.elgoog....	1	0	1	2000	1570909415696000	Fbt9umwCS1...	0
46	https://www.oneplus.com/6t	OnePlus 6T - ...	moc.sulpeno....	1	0	0	100	1570909420163000	wvvoF8t9NH...	0

5. Go through all the emails and write a brief synopsis of who is communicating with whom and what the communications appear to mean

   a. Write your separate document, but no more than 1 full, double-spaced page in total

Laboratory Notes

Laboratory Number: 3 Examiner Name: Akshay Chaurasia

There are two major conversations going on. One is between Jim-Sam (Bike spec's), and the other between Jim-Terry (Bicycle offer). There is another conversation between Terry and **Martha**.

1. **Chicago Tribune & Jim:** Jim receives an email from Chicago Tribune, welcoming him after registering with chicagotribune.com. He is also asked to activate his account using the link provided in the email.
2. **Jim & Bob:** Initially, Bob sent Jim some sensitive documents (spec sheet) which Jim deleted accidently. So, Jim asks Bob to resend the file. Bob resends the file and asks him to rename the file's extension to ".jpg". Bob is asking for $5000 more, which he needs desperately.
3. **Jim & Terry:** Terry is offering $10000 to Jim for the plans to which Jim replies asking for additional 10K. Terry replies to Jim by saying that he cannot provide him $1000 additional but can give him some of it. Jim and Terry also had a telephone call regarding Jim providing Terry with the sample of new product for his clients. Jim then replies asking for some money upfront.
4. **Jim & Sam:** Jim sends the sensitive attachment that he received from Bob to Sam, while asking for down payment. Sam is asking Jim for the investment amount since some investors are ready to pay. Sam says that he/she is ready to pay $4000 for the plans.
5. **Terry & Martha:** Terry sends Martha an email in which he is telling Martha regarding her company that has investor programs and that provides consultation. She also provides the website (www.superiorbicycles.biz) of her company and asks her to check it out.

I think there is something fishy going on. After analyzing the "Outlook Header Information" of the conversation between Terry and Martha, I found out that the receiver of Terry's message is one ***"Bill Nelson"****. So, it looks like that the Martha's account is fake.* It can also be seen that Jim is trying to sell the sensitive file to Sam and Terry. *Also,* ***Jim*** *Shu's outlook data file has two email account, jim_shu@comcast.com and jim_shu1@yahoo.com related to Jim. He is using the comcast email to communicate with* ***Bob****,* ***Terry****,* ***Sam****, and* ***Chicago Tribune*** *and he is using his yahoo account to forward/save emails from his comcast account.*