**Assignment for Facebook Forensics on different OS**

**Prerequisite Forensics tools or software in this assignment:**

1. Virtual Box
2. Linux iso file (<https://drive.google.com/file/d/1uSENWPCWpY2LoL3dDAyW5ZKgqZbZOTgJ/view?usp=sharing>)
3. Windows 7 iso file (<https://drive.google.com/file/d/11C4gsMKUL4ilvUG-BgsRNwKBVhWYUMXk/view?usp=sharing>)
4. Android 9 iso file (<https://drive.google.com/file/d/1izIujKPkY5Ys8R458cw5ecxyte5nscxV/view?usp=sharing>)
5. FTK imager (Optional)
6. Hdx Hex Editor
7. Chrome Browser
8. ChromeCacheView

Q1. Download Linux iso file. Install and setup Linux VM in your Virtual Box. Here’s the instruction you can follow to install Linux VM. (<https://www.lifewire.com/install-ubuntu-linux-windows-10-steps-2202108>)

Please take the screenshot of your Linux VM after you setup successfully.

Q2. Download Android 9.0 iso file. Install and setup Android VM in your Virtual Box. Here’s the instruction you can follow to install Android VM. (<https://www.ehacking.net/2020/04/how-to-install-android-9-0-on-virtualbox-for-hacking.html>)

Also, you need to download and install Facebook app in Android application market.

Please take the screenshot of your Facebook application in Android VM.

Q3. Download Windows 7 iso file. Install and setup Windows 7 VM in your Virtual Box. Here’s the instruction you can follow to install Windows 7 VM. (<https://www.makeuseof.com/tag/installing-windows-7-on-a-virtual-machine/>)

If your Windows 7 VM doesn’t have Chrome Browser, please download it.

Please take the screenshot of your Windows 7 VM after you setup successfully.

Q4. You can do this either on your PC or VMs. This practice is for you to get more familiar with Facebook account and operation. Please clean the Chrome cache before working on this question. Then surf [www.facebook.com](http://www.facebook.com), login into your Facebook account by Chrome web browser. What is your User ID? In this question, this ID is required to be found out from Chrome cache. (Hint: After login into your account, open the ChromeCacheView and search the keyword “\_user=” then you can get the answer) Please take a screenshot to demonstrate it.

Q5. To analyze the forensics evidence, we need to get snapshots of the VMs, and get memory dumps. Which file store the virtual memory dumps of the VM, and what is the extension? Which file is the virtual disk file snapshot, and what is the extension? This step is critical for following questions.

Please get the screenshot of one snapshot of your virtual disk file and memory dump (generally, they should be in the same snapshot file path). And please answer their extensions respectively.

Q6. After you setup the Linux VM in VB, please do following operations in your Linux VM. This step is for creating your Facebook Linux VM dump. Please take screenshot of each following steps.

* 1. Login your Facebook account in browser. If you don’t have a Facebook account, and you don’t have friend to chat, please create two Facebook accounts, one is the main test account and the other is for reply chat message.
  2. Chat to a friend, I recommend to send some words that don’t normally appear in daily life, such as *t1e2s3t*, *nihao\_from\_Linux*, etc.
  3. Post a feed, and reply to yourself, or reply to others posts.
  4. Take a snapshot of your Linux VM and locate the snapshot virtual disk file and memory dump.

Please take a screenshot of your Linux virtual disk snapshot file and memory dump.

Q7. After you setup the Win7 VM in VB, please do following operations in your Win7 VM. This step is for creating your Facebook Win7 VM dump.

* 1. Login your Facebook account in browser.
  2. Chat to a friend, I recommend sending some words that don’t normally appear in daily life, such as *t1e2s3t\_in\_Win*, *nihao\_from\_WIN7*, etc.
  3. Post a feed, and reply to yourself, or reply to others posts.
  4. Take a snapshot of your Win7 VM and locate the snapshot virtual disk file and memory dump.

Please take a screenshot of your Win7 virtual disk snapshot file and memory dump.

Q8. After you setup the Android 9 VM in VB, please do following operations in your Android VM. This step is for creating your Facebook Android VM dump.

* 1. Login your Facebook account in your Facebook app previously downloaded in Q2.
  2. Chat to a friend, I recommend sending some words that don’t normally appear in daily life, such as *t1e2s3t\_in\_android*, *nihao\_from\_AN*, etc. Android OS may need you to download another Facebook Message App to support chatting, please follow the Facebook app instruction and do some chatting in the app.
  3. Post a feed, and reply to yourself, or reply to others posts.
  4. Take a snapshot of your Android VM and locate the snapshot virtual disk file and memory dump.

Please take a screenshot of your Android virtual disk snapshot file and memory dump.

Q9. This step you need to analyze your Linux disk snapshot file and Linux memory dump. Please read the virtual memory of the VM and try to find out the detailed User information of your main test account and login information. Please take screenshots of the information you found in the Virtual disk snapshot file and VM dump memory. Notice you should do the keyword search and the screenshot of the information both in disk snapshot file(.vdi) and Linux memory dump(.sav).

Hint1: You may search keyword like your username, your login email, Facebook URL, etc.

Hint2: The information may not be found or incomplete, try best as you can to find more information of your Facebook account.

Hint3: You could use Hxd Hex Editor or FTK imager or other image memory reader. Perhaps you could use both to discover more information.

Q10. This step you need to analyze your Android disk snapshot file and Android memory dump. Please read the virtual memory of the VM and try to find out the detailed User information of your main test account and login information. Please take screenshots of the information you found in the Virtual disk snapshot file and VM dump memory. Notice you should do the keyword search and the screenshot of the information both in disk snapshot file(.vdi) and Android memory dump(.sav).

Hint1: You may search keyword like your username, your login email, Facebook URL, etc.

Hint2: The information may not be found or incomplete, try best as you can to find more information of your Facebook account.

Hint3: You could use Hxd Hex Editor or FTK imager or other image memory reader. Perhaps you could use both to discover more information.

Q11. This step you need to analyze your Windows 7 disk snapshot file and Win7 memory dump. Please read the virtual memory of the VM and try to find out the detailed User information of your main test account and login information. Please take screenshots of the information you found in the Virtual disk snapshot file and VM dump memory. Notice you should do the keyword search and the screenshot of the information both in disk snapshot file(.vdi) and Android memory dump(.sav).

Hint1: You may search keyword like your username, your login email, Facebook URL, etc. In Win7, you may find a huge user information difference comparing two other OS. If you found something, please also write your finding and thoughts in your answer.

Hint2: The information may not be found or incomplete, try best as you can to find more information of your Facebook account.

Hint3: You could use Hxd Hex Editor or FTK imager or other image memory reader. Perhaps you could use both to discover more information.

Q12. This step you need to analyze your chatting operation of Linux disk snapshot file and Linux memory dump. Please try to find information of the chat in Facebook. Please take screenshots of the information you found in the Virtual disk snapshot file and VM dump memory.

Hint1: You may search keyword like your chat friend name, your chatting content, *messaging\_actor*, etc.

Hint2: The information may not be found or incomplete, try best as you can to find more information of your Facebook account. If you find nothing, please also take the screenshot.

Q13. This step you need to analyze your chatting operation of Android disk snapshot file and Android memory dump. Please try to find information of the chat in Facebook. Please take screenshots of the information you found in the Virtual disk snapshot file and VM dump memory.

Hint1: You may search keyword like your chat friend name, your chatting content, *messaging\_actor*, etc.

Hint2: The information may not be found or incomplete, try best as you can to find more information of your Facebook account. If you find nothing, please also take the screenshot.

Q14. This step you need to analyze your chatting operation of Win7 disk snapshot file and Win7 memory dump. Please try to find information of the chat in Facebook. Please take screenshots of the information you found in the Virtual disk snapshot file and VM dump memory.

Hint1: You may search keyword like your chat friend name, your chatting content, *messaging\_actor*, etc.

Hint2: The information may not be found or incomplete, try best as you can to find more information of your Facebook account. If you find nothing, please also take the screenshot.

Q15: Please compare the information you got from question9 to question14, talk about your thoughts on the Facebook forensics evidence difference among these three operating systems.