

Security Analysis, Techniques and procedures

Lab 6a

Wales Institute of Science and Art
Applied Computing
I.Q Building, Room 205
Swansea
SA1 8EW

Introduction

The Computer Forensics investigation is a methodological approach of preparing for an investigation, collecting and analyzing digital evidence. It is also managing the case from the reporting of the crime till the case's conclusion. The process takes place in a computer forensic lab.

Computer forensics plays a vital role in the investigation and prosecution of cyber criminals. The process includes acquisition, inspection, and reporting of information stored across computers and networks related to a civil or criminal incident. Forensic investigators are trained professionals who can extract, analyze, report, and investigate cases that involve technology as the source or the victim of a crime.

As a computer forensics investigator, it is important to have knowledge of the process involved during a forensics investigation, such as collecting digital evidence, building a computer forensics lab, recovering the deleted data, etc.

Task 1:

- Sign in **www.tryhackme.com**
- Go to Hackactivities → select free only from the **show** pop down list → walkthrough from the **Type** pop down list.
- Select **Forensics** and attempt a lab of your choice. Each week try to complete a different one.

Task 2: Analysing Domain and IP address queries using SmartWhois Tool

SmartWhois is a network information utility that allows you to look up the most available information on a hostname, IP address, or domain.

Lab Scenario

To be an expert **forensic investigator**, you must be able to analyze and resolve queries related to domain addresses.

Lab Objectives

Jack has filed a complaint that somebody is remotely accessing his system and hacking his accounts. During investigation, the forensic officer with the help of SmartWhois tool analyzes the attacker's IP address and finds the domain used.

The objective of this lab is to help investigators analyze domain and IP address queries. It will help you to get most available information on a hostname, IP address, and domain.

Lab Environment

To carry out the lab, you need:

- SmartWhois tool, located at: https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EkEaN-DK6dAJHquJ8HSRt4BgBTSQEmSEeGjoZHI_jeu3PmQ?e=5zhkrP
- You can also download the latest version of **SmartWhois** from www.tamos.com/download/main.
- If you are willing to download the latest version of **SmartWhois**, screenshots shown in the lab might differ.
- A computer running on **Windows Server 2012**.
- Administrative privileges to run tools.
- A web browser with an **Internet** connection.

Overview of SmartWhois

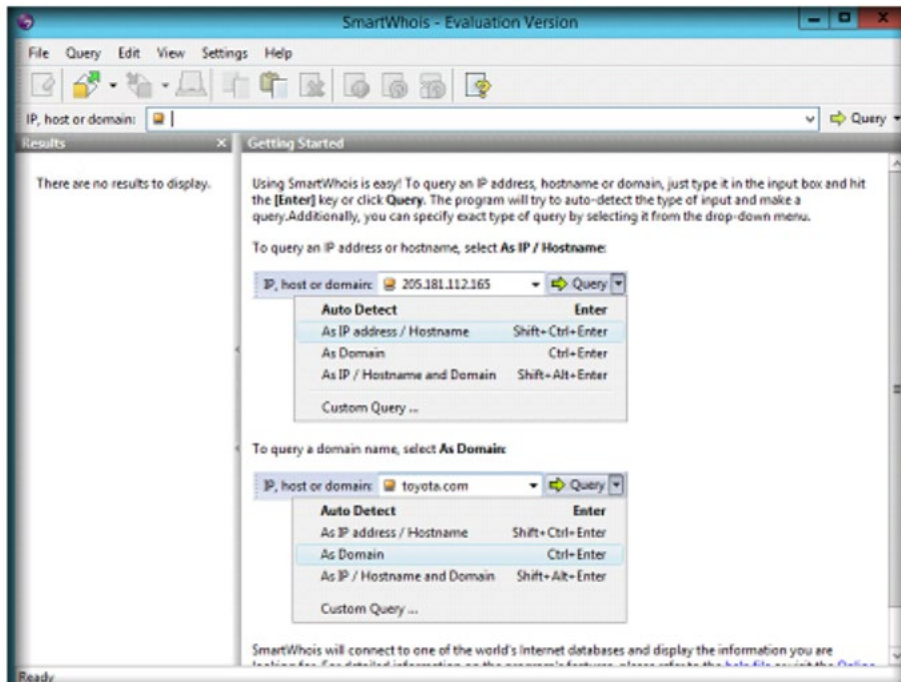
SmartWhois is a useful network information utility that allows you to look up all the available information about an **IP address, hostname, or domain**, including country, state or province, city, name of the network provider, administrator, and technical support contact information. It helps you to find answers to the following important questions:

- Who is the owner of the domain?
- When was the domain registered, and what is the owner's contact information?
- Who is the owner of the IP address block?

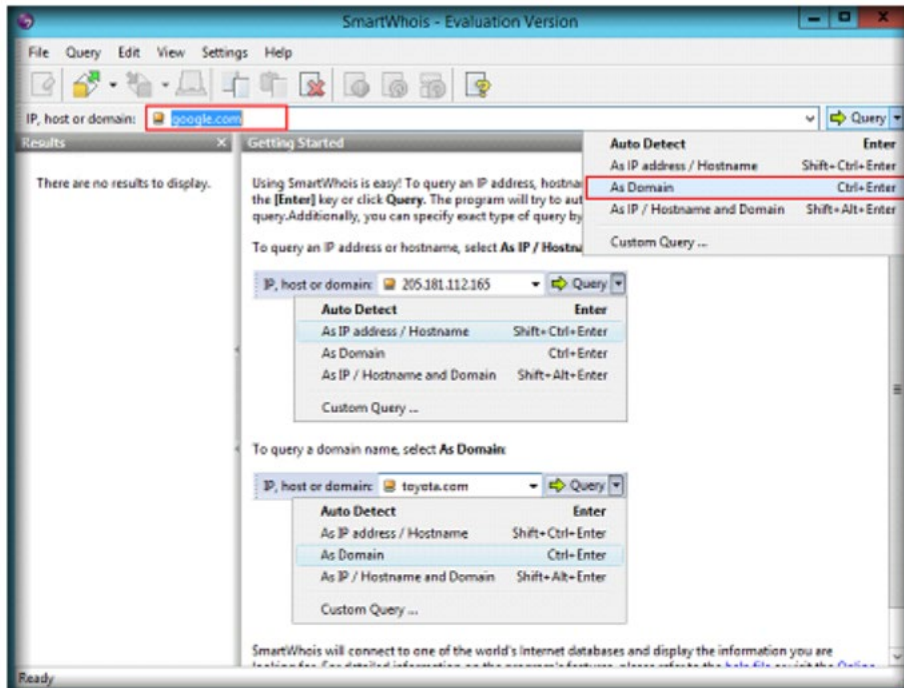
Lab Tasks

1. Navigate to https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EkEaNDK6dAJHquJ8HSRt4BgBTSQEmSEeGjoZHI_jeu3PmQ?e=5zhkrP
2. Double-click **setup.exe** to launch the setup and follow the wizard-driven installation instructions.
3. Double-click the Desktop shortcut to launch **SmartWhois** tool.

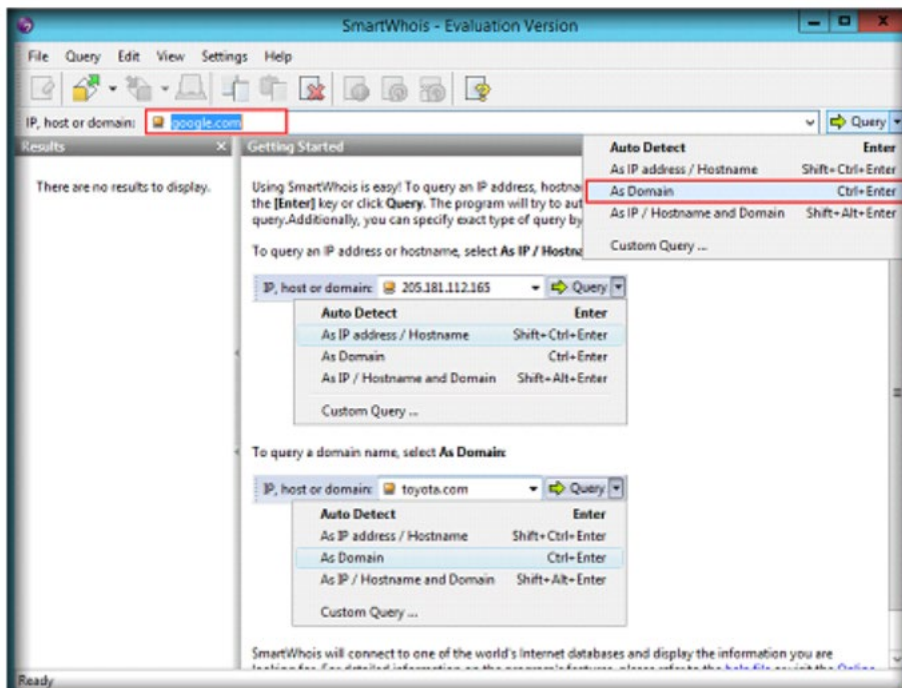
Note: You can launch the tool from the Apps screen of the system.



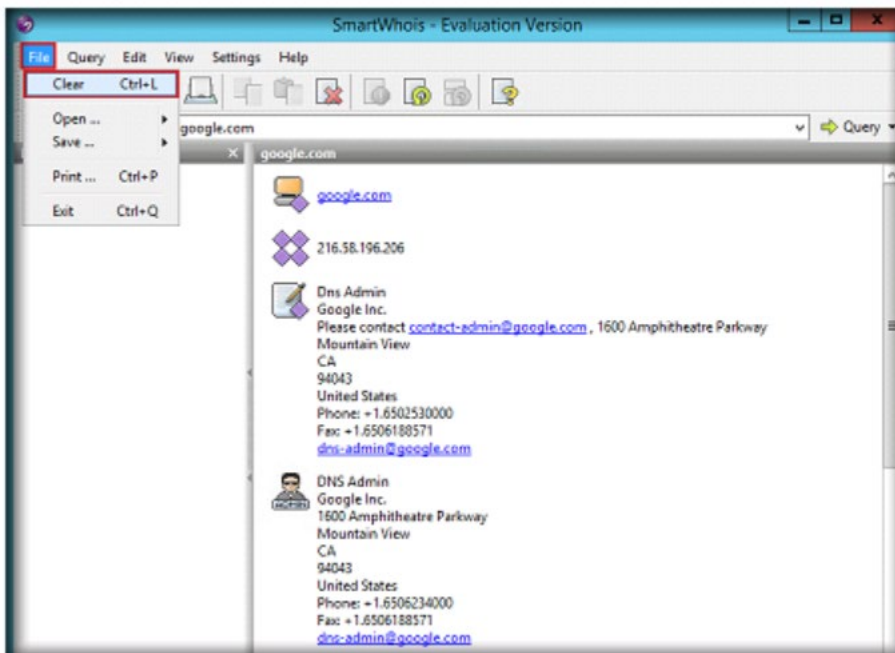
4. To perform a domain name query, type a domain name in the **IP, host or domain** field. Click the **Query** drop-down menu and select **As Domain**. Consider **www.google.com** as an example for domain name query.



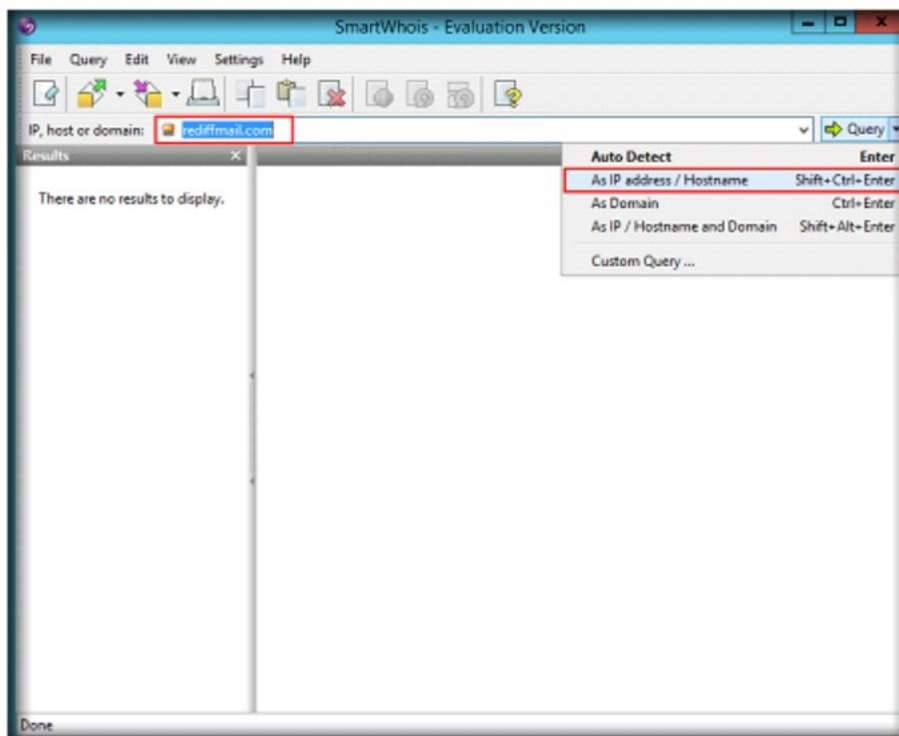
5. **SmartWhois** will process the query and display the results.



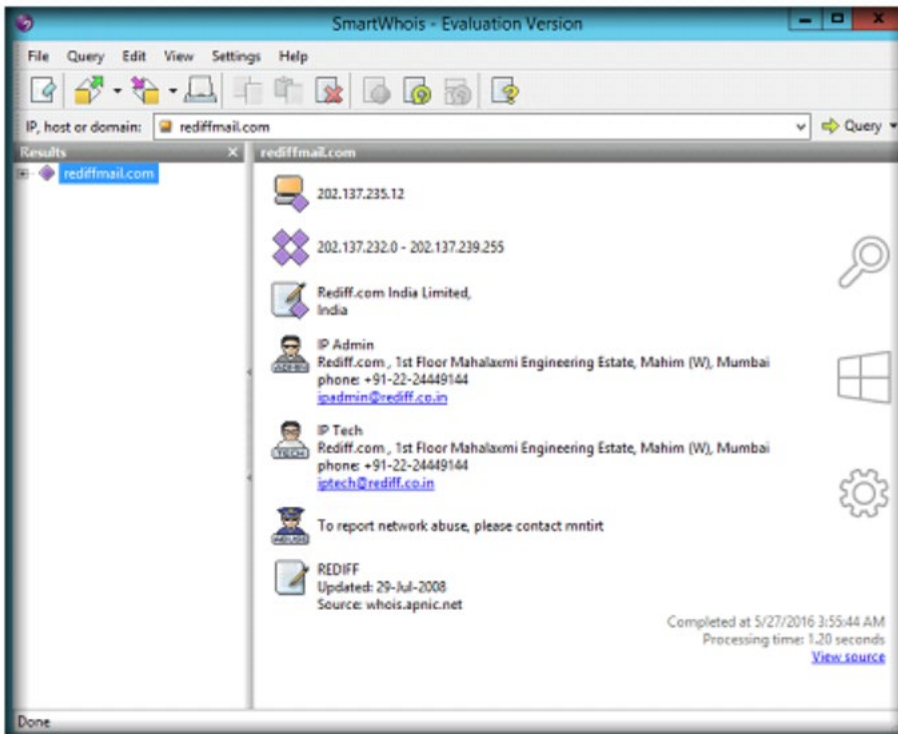
6. Navigate to **File → Clear** in the menu bar to clear the history.



7. To perform a hostname query, type a hostname in the **IP, host or domain** field. Click the **Query** drop-down menu and select **As IP address/Hostname**. Consider **www.rediffmail.com** as an example for hostname query.

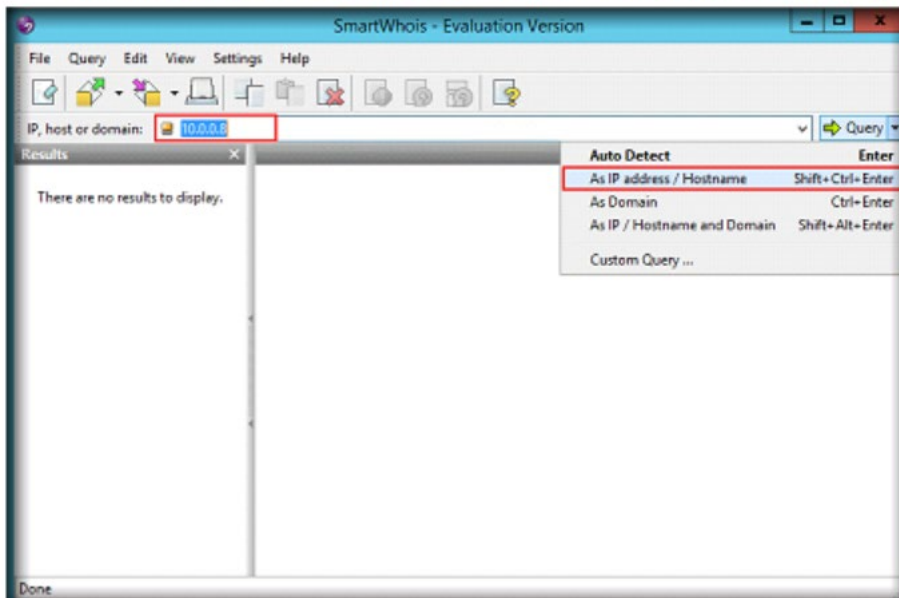


8. **SmartWhois** will process the query and display the results.

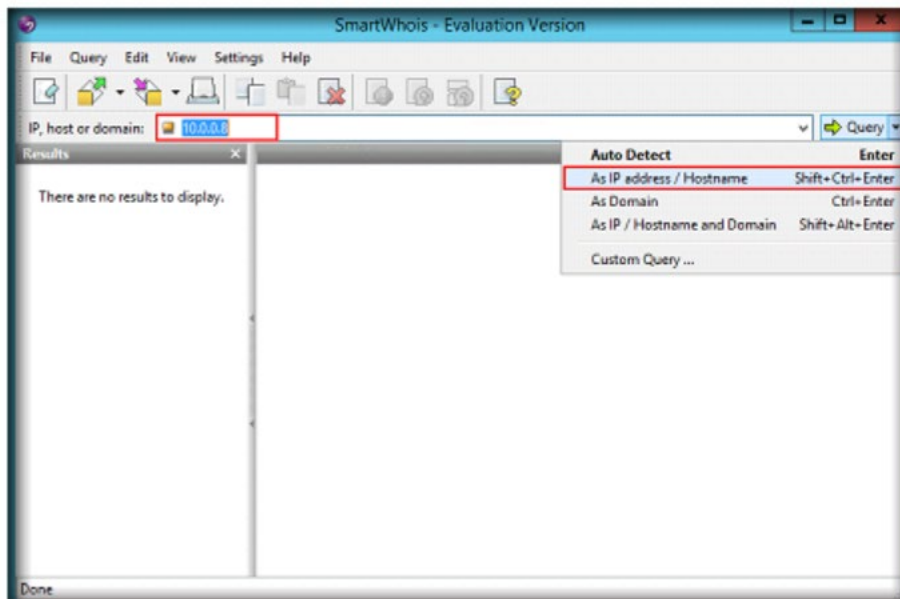


Note: You can perform another query with or without clearing the history.

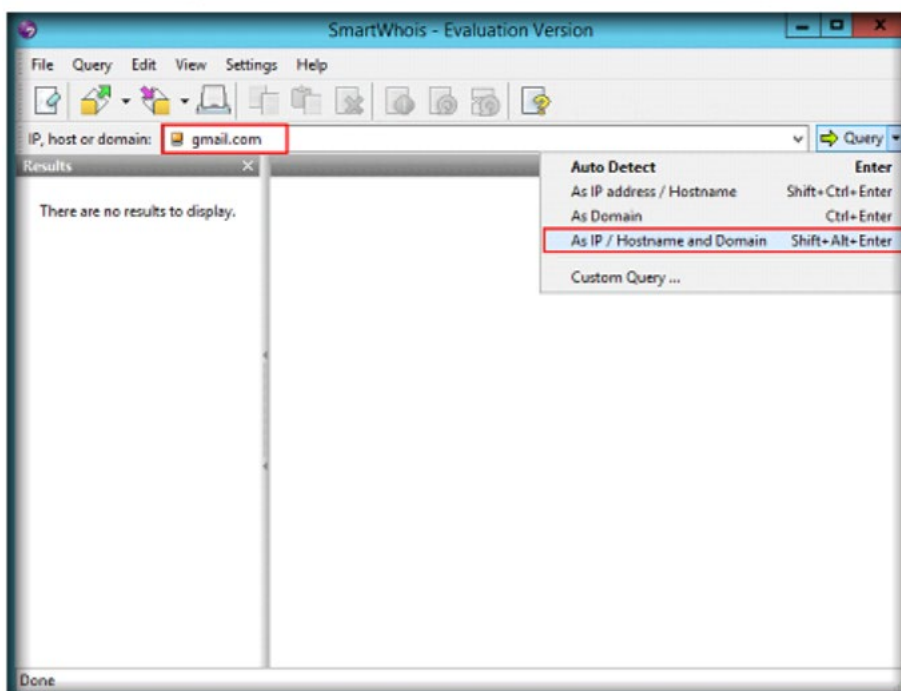
9. To perform an IP address query, type an IP address in the **IP, host or domain** field. Click the **Query** drop-down menu and then select **As IP address/Hostname**. Consider **10.0.0.8** as an example for IP address query.



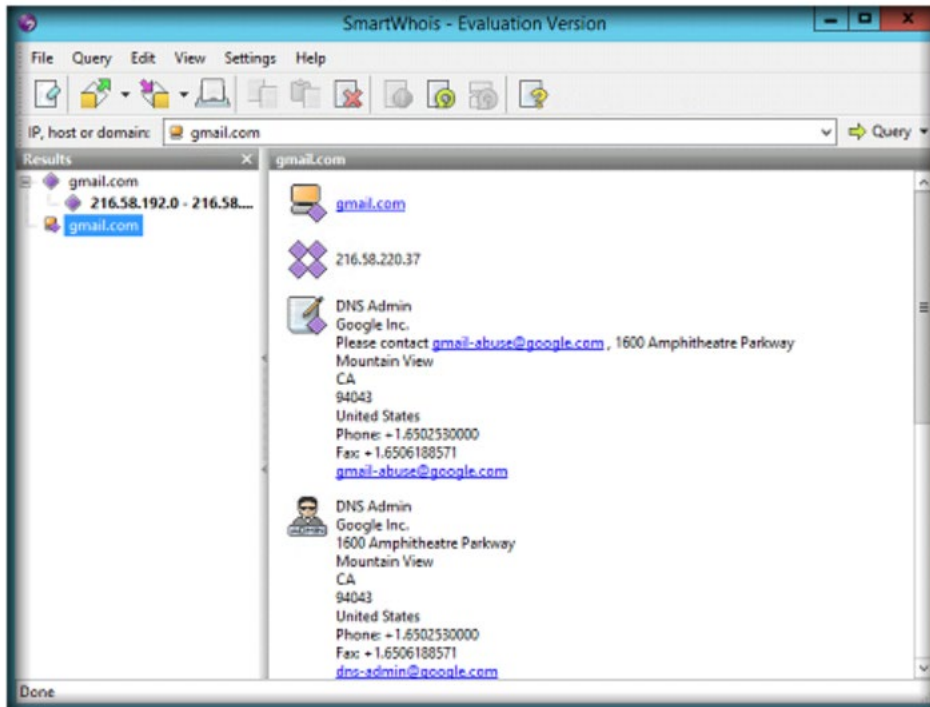
10. **SmartWhois** will process the query and display the results.



11. To perform the IP address/hostname and domain name query all together, type the target **website address** in the field. Click the **Query** drop-down menu and select **As IP /Hostname and Domain**. Consider **www.gmail.com** as an example for IP address/hostname and domain name query.

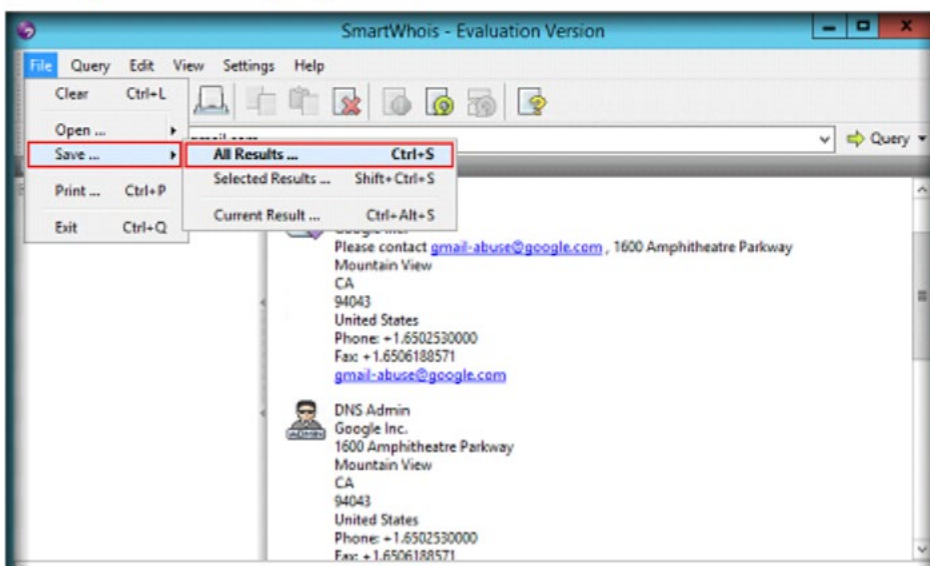


12. **SmartWhois** will process the query and display the results. In the **left pane** of the window, the result displays, and in the **right pane**, the text area displays the results of your query.

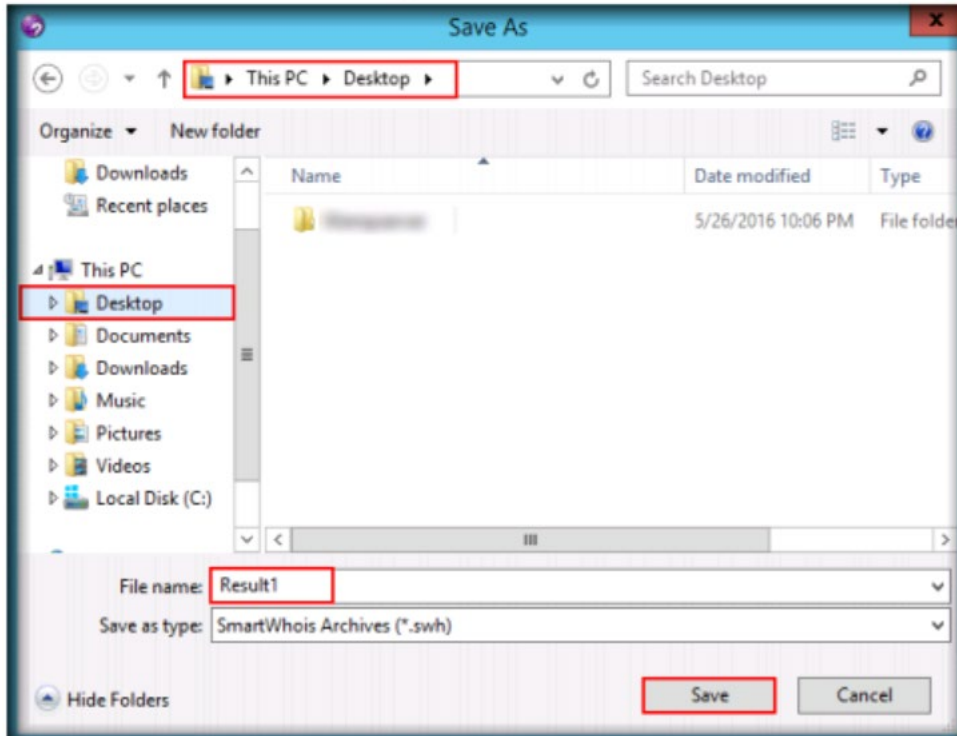


Note: To see the results of domain name or host name query, switch among the results displayed in the left pane of the window.

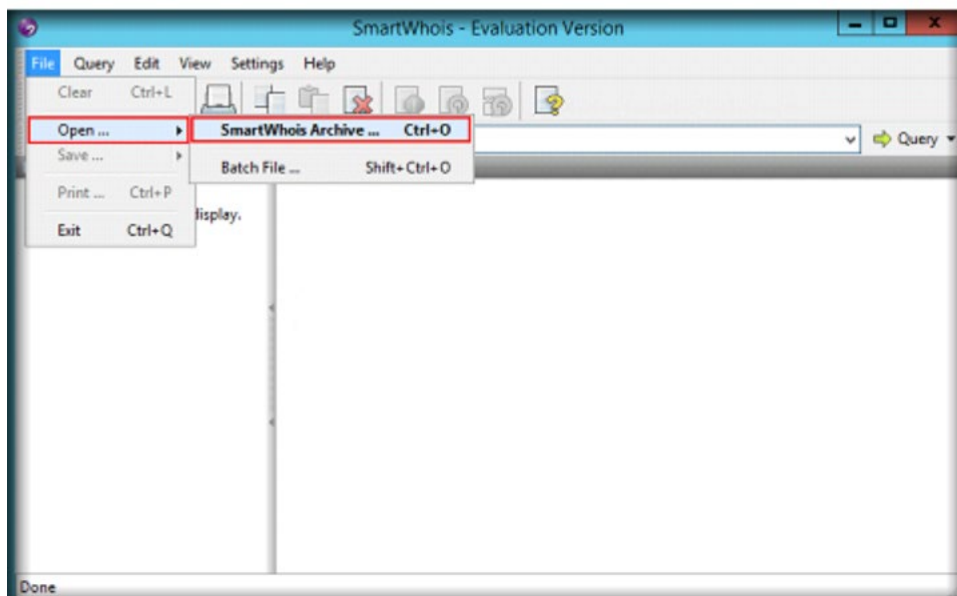
13. You can also save the results for future reference. To save the results, go to **File → Save** and select **All Results....** It will display the options. Choose the options according to your requirement.



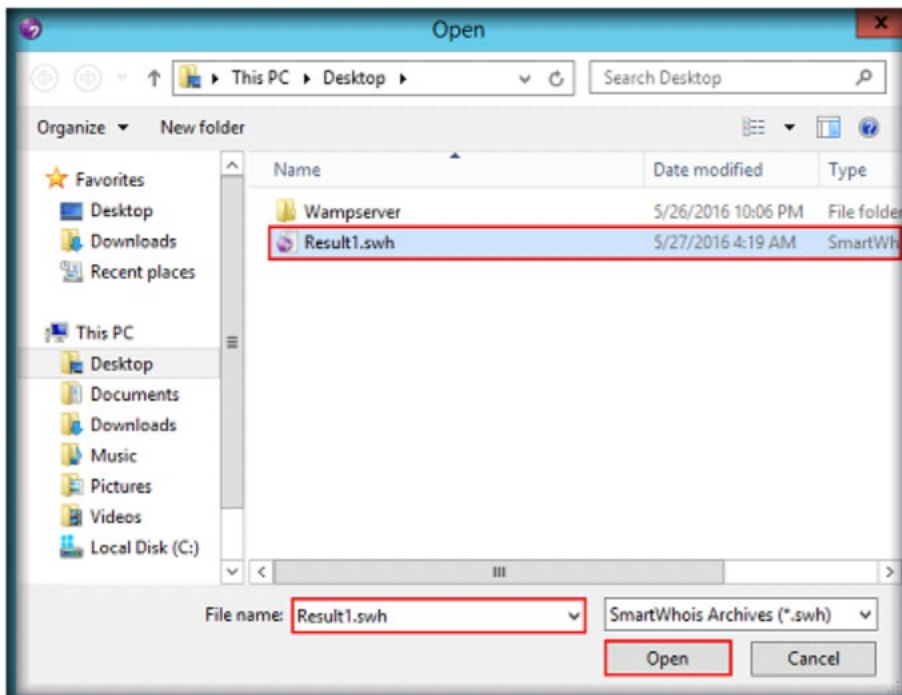
14. **Save As** window appears, browse the location where you want to save the file, type the **file name** for the results, and click the **Save** button. (Here, we selected **Desktop** for saving the file.)



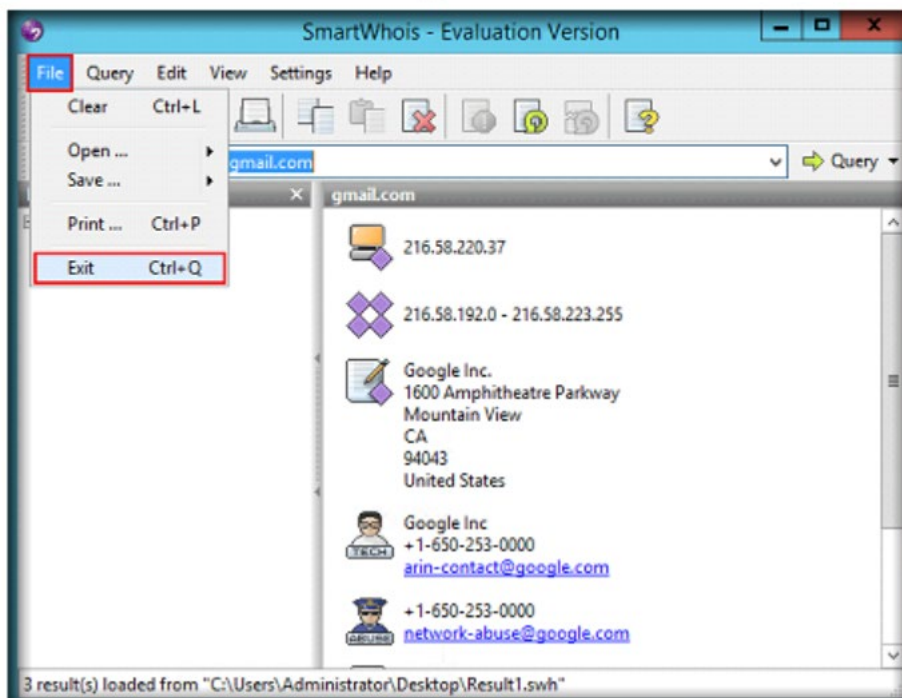
15. To open the saved results' document, go to **File → Open → SmartWhois Archive...**



16. **Open** window appears, browse the location where you saved the results, select the file, and then click **Open**.



17. To close the **SmartWhois** tool, go to **File → Exit**.



Lab Analysis

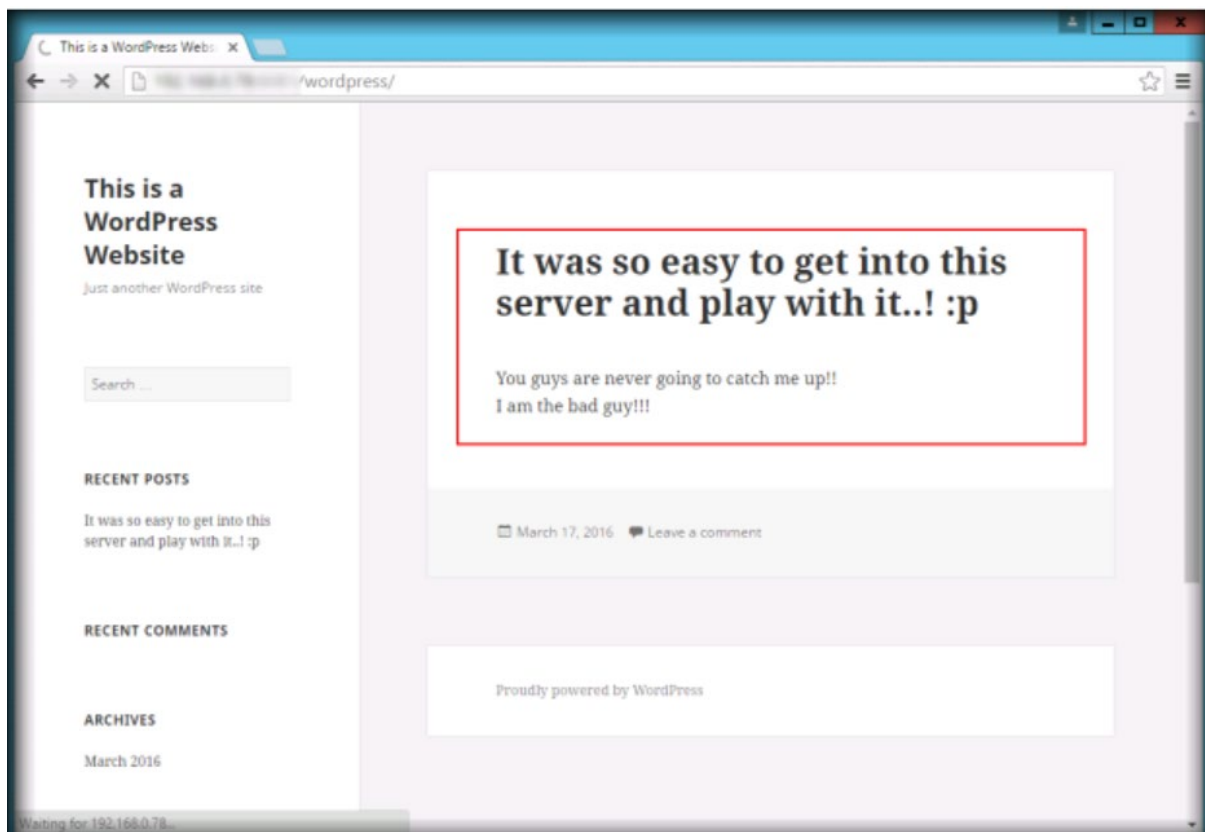
Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

Task 3: Performing Forensic Investigation on a MySQL Server Database

MySQL is an open-source relational database management system for use in web applications.

Lab Scenario

A suspicious post was found on a WordPress website's homepage, which indicates that a suspicious activity has occurred on the backend database. The objective of this lab is to find the malicious user who gained access to **mysql** server and examine the activities performed by him/her on the database named **WordPress**.



Lab Objectives

In this lab, you will learn how to examine the databases and find the transactions performed by a suspicious user.

Lab Environment

This lab requires:

- A **Windows Server 2012** virtual Machine
- Hex Workshop Hex Editor located at https://uwotds-my.sharepoint.com/:f/g/personal/carlene_campbell_uwotds_ac_uk/Eh2ghZl64KFMqcGfEB7qcTgBBaQ4kQfXIF3CZ8V9L3DWNQ?e=WbSDnZ
- WampServer located at https://uwotds-my.sharepoint.com/:f/g/personal/carlene_campbell_uwotds_ac_uk/Eh2ghZl64KFMqcGfEB7qcTgBBaQ4kQfXIF3CZ8V9L3DWNQ?e=WbSDnZ
- Microsoft Visual C++ 2012 located at https://uwotds-my.sharepoint.com/:f/g/personal/carlene_campbell_uwotds_ac_uk/Eh2ghZl64KFMqcGfEB7qcTgBBaQ4kQfXIF3CZ8V9L3DWNQ?e=WbSDnZ
- Administrative privileges to run the tools

Overview of the Lab

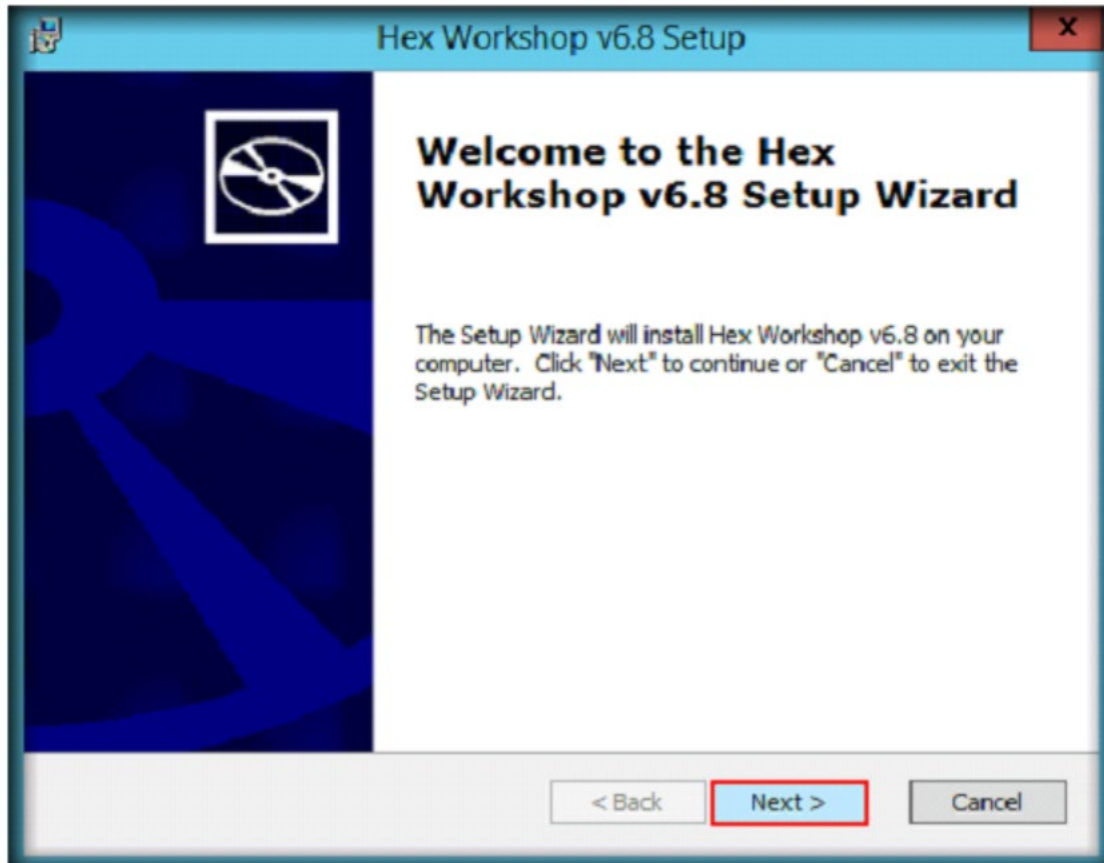
- Install the **WampServer** and understand its working.
- Use **Hex Workshop Hex Editor** to find the hidden evidence files from the database.

Lab Tasks

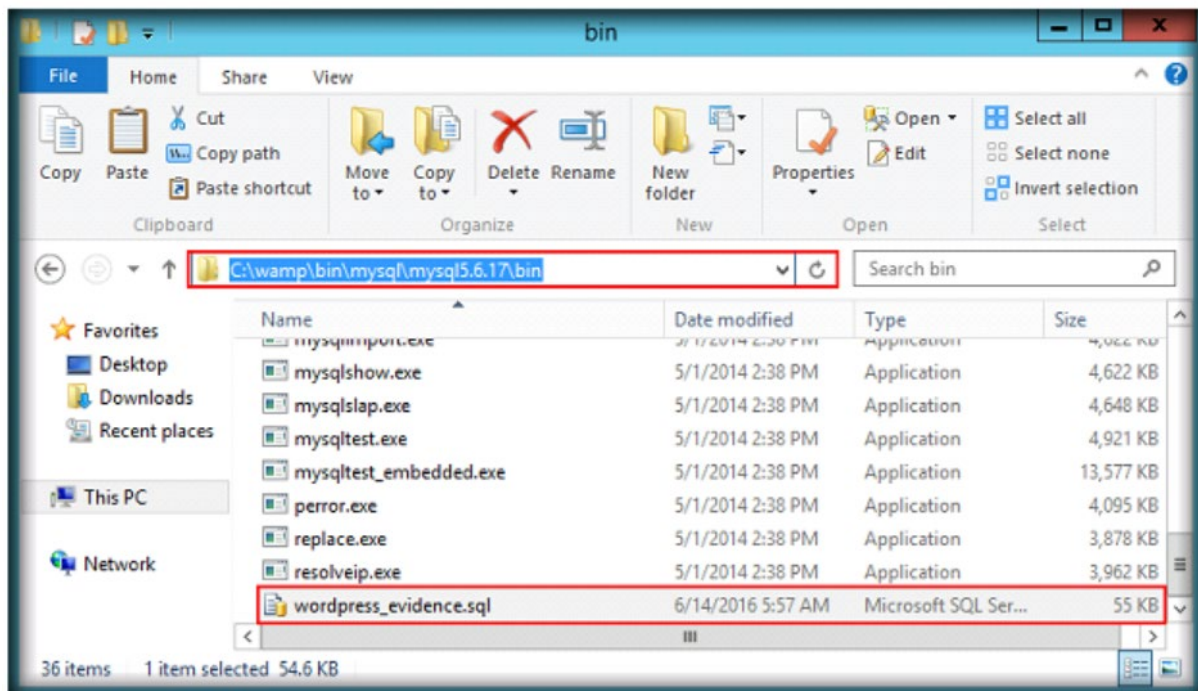
1. Before beginning this lab, you need to logon to **Windows Server 2012** virtual machine.
2. Navigate to https://uwotds-my.sharepoint.com/:f/g/personal/carlene_campbell_uwotds_ac_uk/Eh2ghZl64KFMqcGfEB7qcTgBBaQ4kQfXIF3CZ8V9L3DWNQ?e=WbSDnZ

3. Follow the wizard-driven installation steps to install the application.

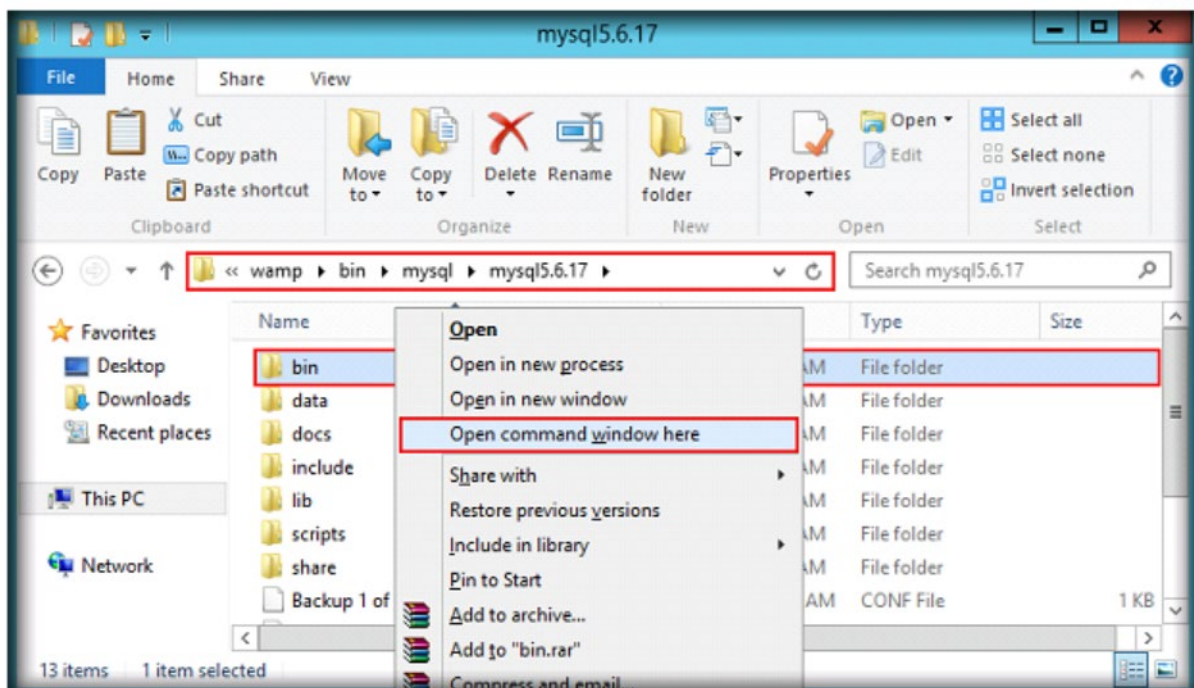
Note: If **Open File - Security Warning** pop-up appears, click **Run**.



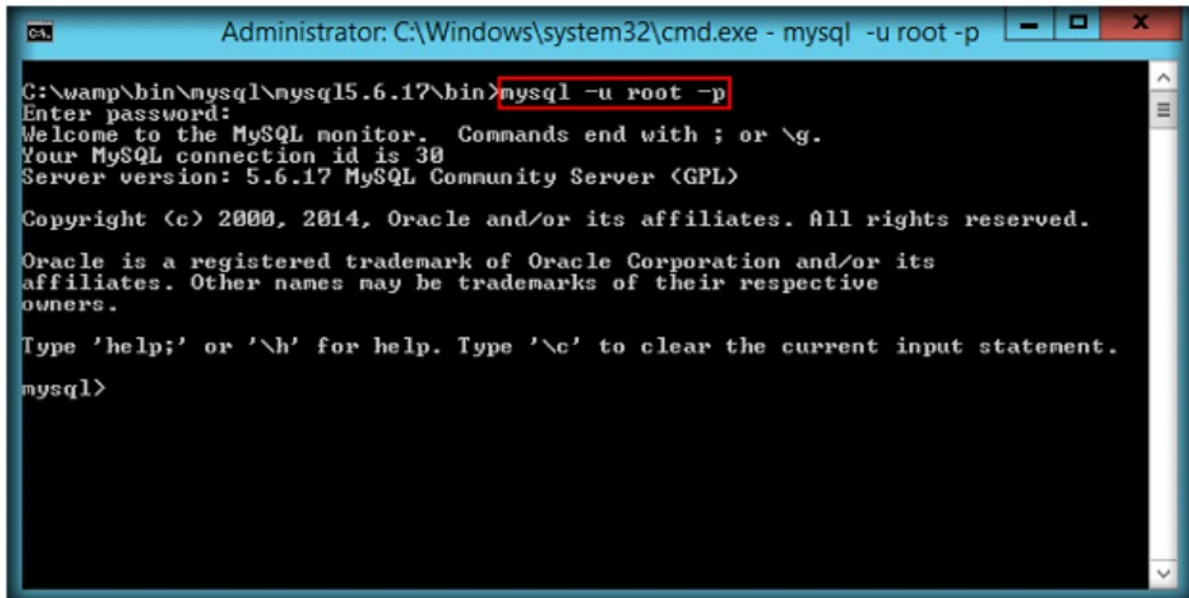
4. On completion of installation, if an **Installer Information** dialog-box appears, click **Yes** to restart the virtual machine.
5. On installing the applications, navigate to https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/Eh2ghZl64KFMqcGfEB7qcTgBBaQ4kQfXIF3CZ8V9L3DWNQ?e=WbSDnZ



6. Now, navigate to **C:\wamp\bin\mysql\mysql5.6.17**, select **bin** folder, press **Shift** on the keyboard and right-click on the folder. Context menu appears. Select **Open command window here**.



7. Command prompt appears. Point the location of **bin** folder. Type **mysql -u root -p** and press **Enter**. You will be asked to enter password. In the **Enter password** field, press **Enter** without issuing any password.
8. A mysql shell appears as shown in the following screenshot:



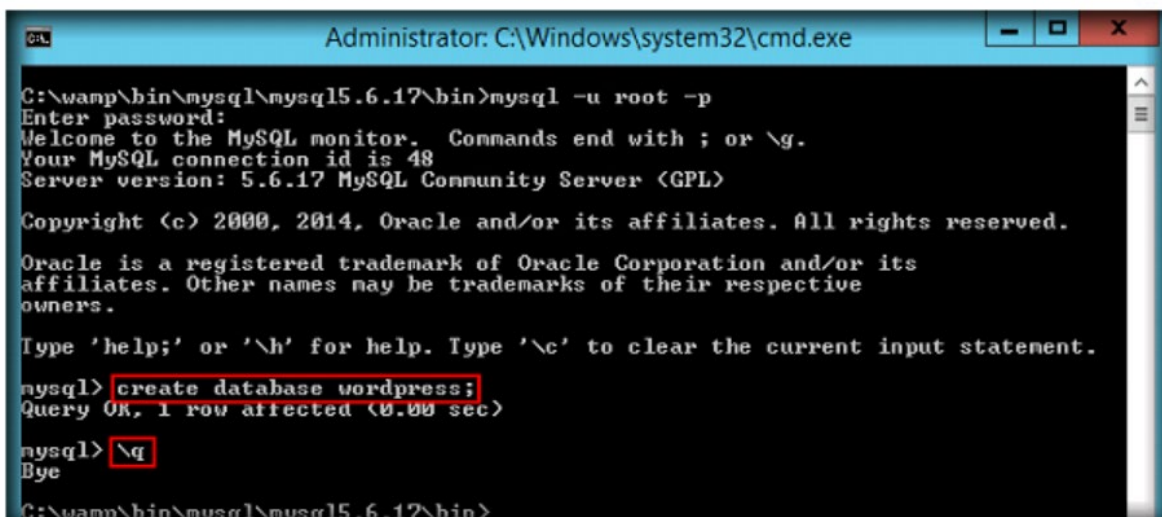
```
Administrator: C:\Windows\system32\cmd.exe - mysql -u root -p
C:\wamp\bin\mysql\mysql5.6.17\bin>mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 30
Server version: 5.6.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql>
```

9. Type **create database wordpress;** in the shell and press **Enter**. This creates a database named **wordpress**. Once done, type **\q** and press **Enter** to come out of the mysql shell.



```
Administrator: C:\Windows\system32\cmd.exe
C:\wamp\bin\mysql\mysql5.6.17\bin>mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.6.17 MySQL Community Server (GPL)

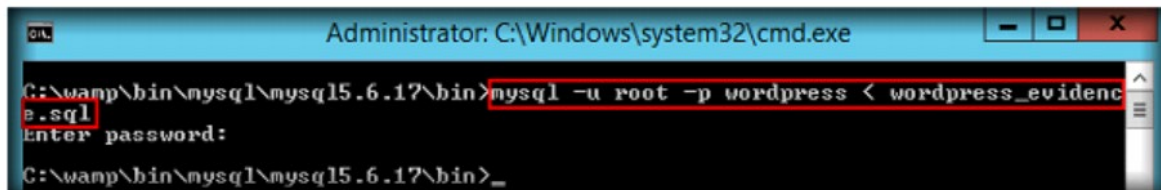
Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> create database wordpress;
Query OK, 1 row affected (0.00 sec)

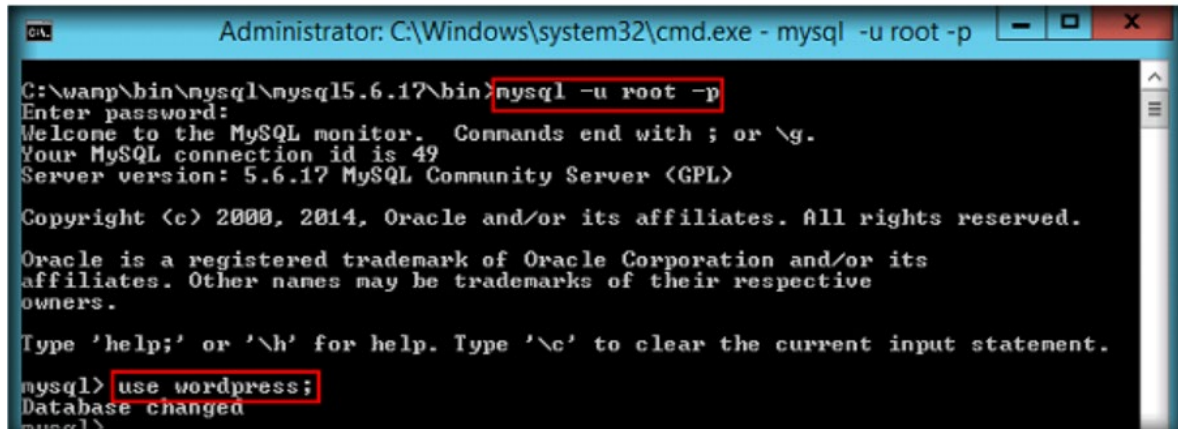
mysql> \q
Bye
C:\wamp\bin\mysql\mysql5.6.17\bin>
```

10. Now, we shall copy all the contents of the dump file to the newly created database.
11. To copy, type **mysql -u root -p wordpress < wordpress_evidence.sql** in the command prompt and press **Enter**.
12. You will be asked to enter password. In the **Enter password** field, press **Enter** without issuing any password.



```
Administrator: C:\Windows\system32\cmd.exe
C:\wamp\bin\mysql\mysql5.6.17\bin>mysql -u root -p wordpress < wordpress_evidence.sql
Enter password:
C:\wamp\bin\mysql\mysql5.6.17\bin>
```

13. Once the backup is copied to the database, we shall login to mysql shell and (by entering **mysql -u root -p** and then issuing **empty password**) start examining the database. To examine the database, we need to use the database.
14. Type **use wordpress;** and press **Enter** to use the **wordpress** database.



```
Administrator: C:\Windows\system32\cmd.exe - mysql -u root -p
C:\wamp\bin\mysql\mysql5.6.17\bin>mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 49
Server version: 5.6.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use wordpress;
Database changed
mysql>
```

15. Now, we shall view the tables in this database. To view, type **show tables;** and press **Enter**.

```

Administrator: C:\Windows\system32\cmd.exe - mysql -u root -p
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use wordpress;
Database changed
mysql> show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta      |
| wp_comments         |
| wp_links            |
| wp_options          |
| wp_postmeta         |
| wp_posts            |
| wp_term_relationships |
| wp_term_taxonomy   |
| wp_terms            |
| wp_usermeta         |
| wp_users            |
+-----+
11 rows in set (0.00 sec)

mysql>

```

16. The **wp_users** table contains all the users accounts associated with the wordpress website. To view the users, type **select * from wp_users;** and press **Enter**.

```

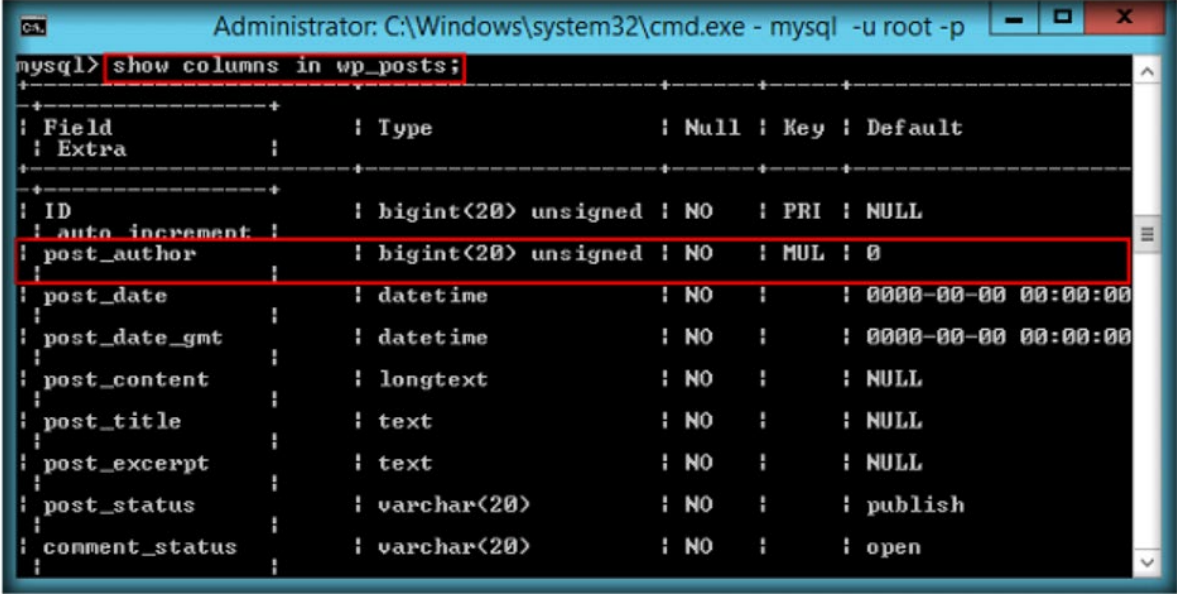
Administrator: C:\Windows\system32\cmd.exe - mysql -u root -p
mysql> select * from wp_users;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_status | display_name | activation_key | user |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | $P$BSScenYvM0uAldinorZLM7Qd0kZA0k/ | admin | in@abc.com | http://www.admin.com | 0000-00-00 00:00:00 | 0 | Admin | 0 | admin |
| 2 | james | ceb6c970658f31504a901b89dcd3e461 | james | esfaulkner@gmail.com | http://www.jameswebsite.com | 0000-00-00 00:00:00 | 0 | jamesfaulkner | 0 | james |
| 125 | bad_guy | $P$B.0WVYbJl0s0yP2EYS.b6.d0xnkBKe/ | anonymous_hacker | bad_guy@xyz.com |  | 0000-00-00 00:00:00 | 0 |  | 0 | bad_guy |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>

```

17. It is observed that a suspicious user account with the username **bad_guy** is present in the table. Make a note of the user ID which is **125**.

18. Since the scenario in the beginning of the lab states that a suspicious post was found on the webpage, we shall view the columns in **wp_posts** table. To view the columns, type **show columns in wp_posts;** and press **Enter**.



The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\system32\cmd.exe - mysql -u root -p". The prompt is "mysql> show columns in wp_posts;". The output is a table with columns: Field, Type, Null, Key, and Default. The rows are: ID (bigint(20) unsigned, NO, PRI, NULL), post_author (bigint(20) unsigned, NO, MUL, 0), post_date (datetime, NO, 0000-00-00 00:00:00), post_date_gmt (datetime, NO, 0000-00-00 00:00:00), post_content (longtext, NO, NULL), post_title (text, NO, NULL), post_excerpt (text, NO, NULL), post_status (varchar(20), NO, publish), and comment_status (varchar(20), NO, open). The row for post_author is highlighted with a red box.

```
mysql> show columns in wp_posts;
+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default |
+-----+-----+-----+-----+-----+
| ID | bigint(20) unsigned | NO | PRI | NULL |
| post_author | bigint(20) unsigned | NO | MUL | 0 |
| post_date | datetime | NO |  | 0000-00-00 00:00:00 |
| post_date_gmt | datetime | NO |  | 0000-00-00 00:00:00 |
| post_content | longtext | NO |  | NULL |
| post_title | text | NO |  | NULL |
| post_excerpt | text | NO |  | NULL |
| post_status | varchar(20) | NO |  | publish |
| comment_status | varchar(20) | NO |  | open |
+-----+-----+-----+-----+-----+
```

19. You will observe a column named **post_author**, which corresponds to the posts made by the users.
20. Now, using **post_author** and the user id of **bad_guy**, we can collect all the posts made by the suspicious user (bad_guy).
21. Issue the following commands to collect the posts:

```
select * from wp_posts
where post_author = '125'
into outfile 'evidence.txt';
```

```
mysql> select * from wp_posts
-> where post_author = '125'
-> into outfile 'evidence.txt';
Query OK, 3 rows affected (0.00 sec)
mysql> _
```

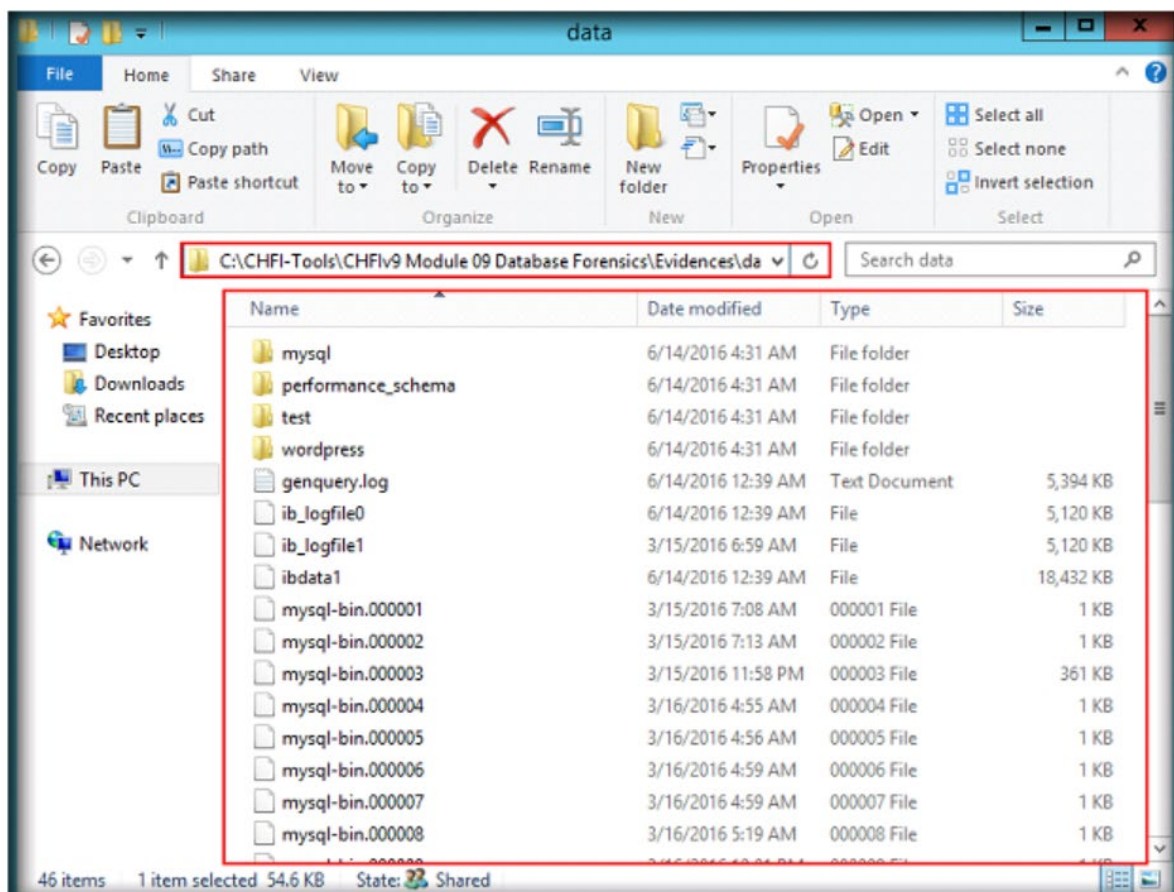
22. By issuing the above commands, the posts made by the user whose ID is **125** are collected, and saved to a file named **evidence.txt** in the location **C:\wamp\bin\mysql\mysql5.6.17\data\wordpress**.
23. Now, navigate to this location and open the file. You will observe all the posts made by the user as shown in the following screenshot:

```
1 125 2016-06-14 07:34:10 0000-00-00 00:00:00 Auto Draft auto-draft open
open 2016-06-14 07:34:10 0000-00-00 00:00:00 0
http://192.168.0.78:8081/wordpress/?p=2 0 post 0
2 10 125 2016-06-14 07:38:52 2016-06-14 07:38:52 It was so easy to hack into the web application. Never
thought it would be such easy to get into this!!! Never thought this would happen publish
open open never-thought-this-would-happen 2016-06-14 07:38:59 2016-06-14
07:38:59 0 http://192.168.0.78:8081/wordpress/?p=10 0 post 0
3 11 125 2016-06-14 07:38:52 2016-06-14 07:38:52 It was so easy to hack into the web application. Never
thought it would be such easy to get into this!!! Never thought this would happen inherit
open open 10-revision-v1 2016-06-14 07:38:52 2016-06-14 07:38:52 10
http://192.168.0.78:8081/wordpress/?p=11 0 revision 0
```

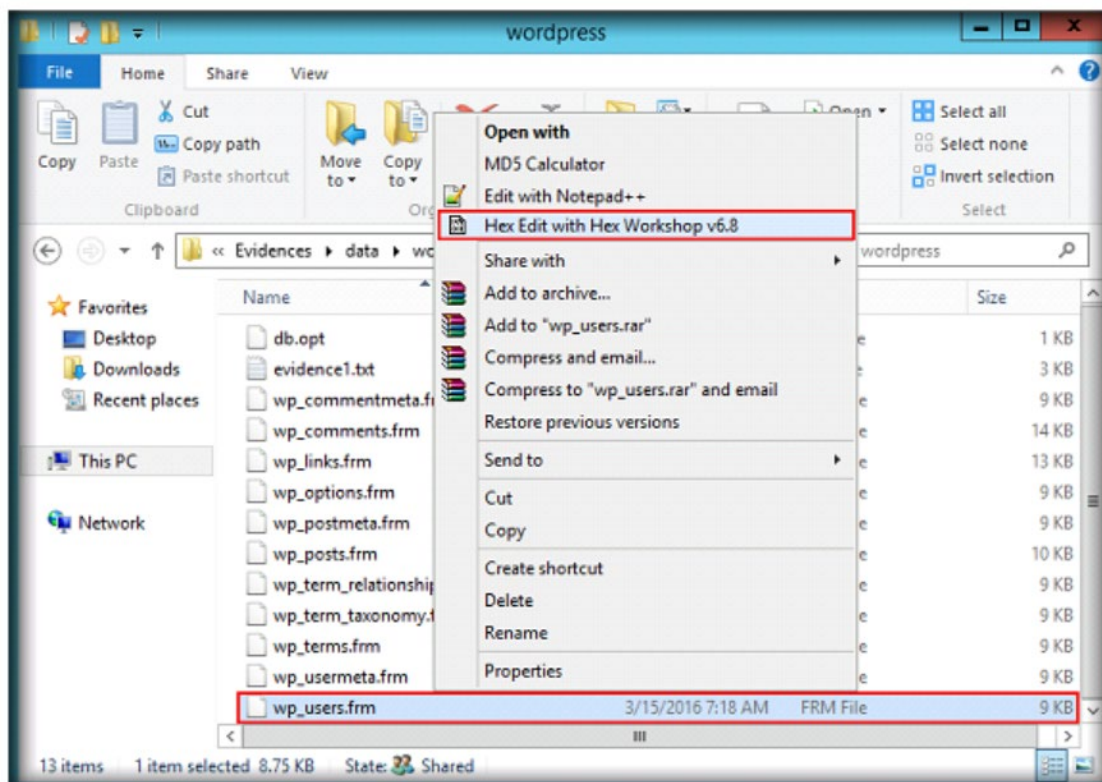
24. Now, we shall track events performed by the malicious user (MyISAM Storage Engine) and recover the deleted data.

25. The binary log files store all the transactions occurred on the databases. An investigator can examine these files to track the events performed by a particular user on the target database.

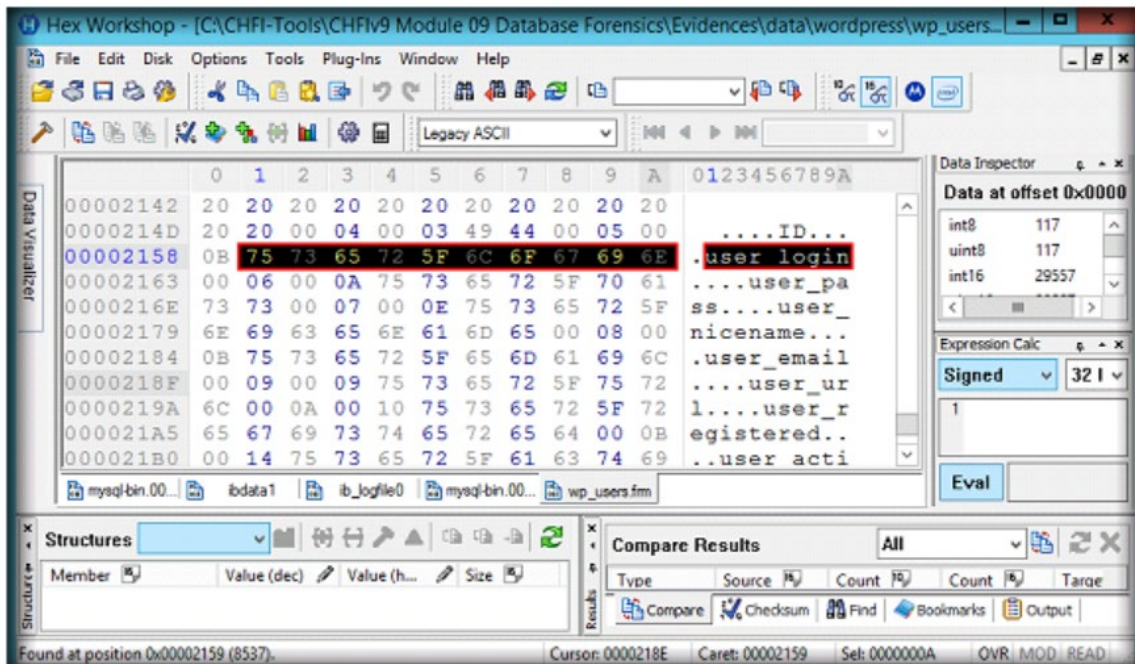
26. Navigate to https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/Eh2ghZl64KFMqcGfEB7qcTgBBaQ4kQfXIF3CZ8V9L3DWNQ?e=WbSDnZ. You will find all the logs associated with the database as shown in the following screenshot.



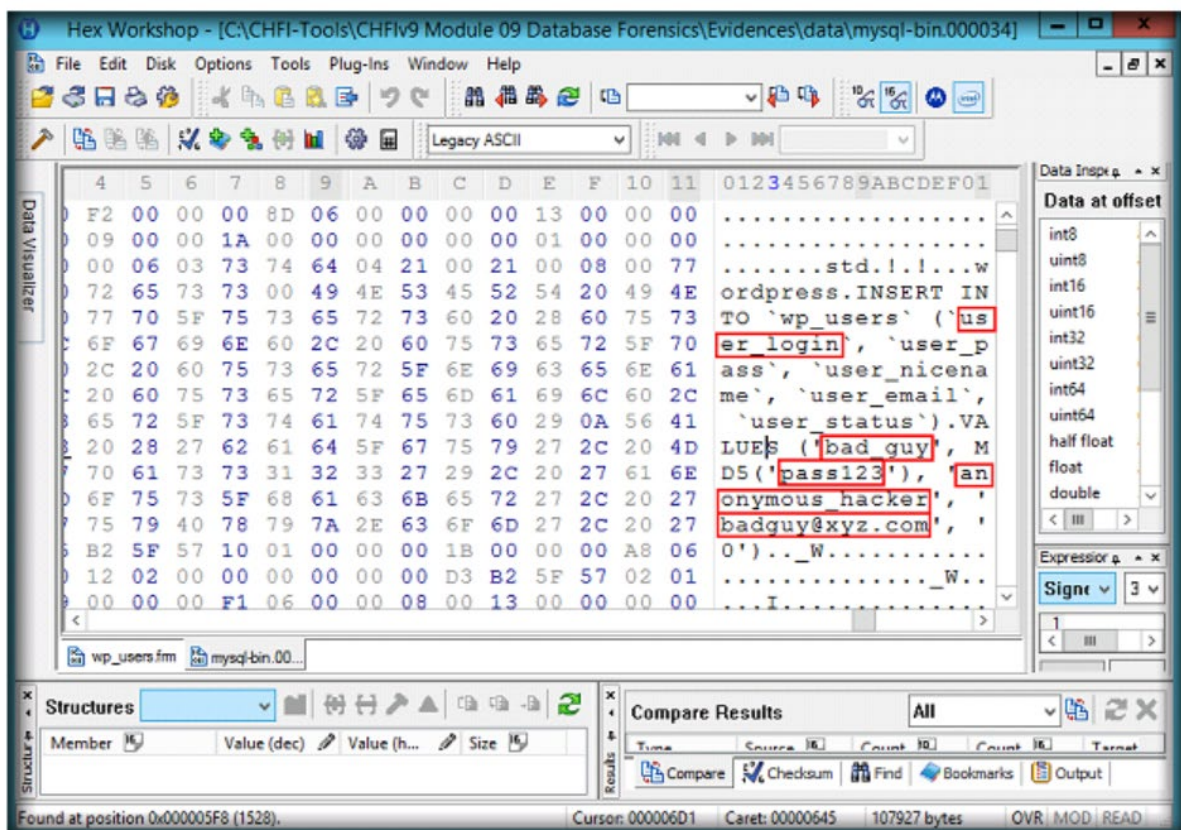
27. Analyzing the **.frm** files helps a forensic examiner to understand the table format and the terms related to the table content.
28. Since the malicious user created a user account for himself with the login name **bad_guy**, you may analyze the **wp_users.frm** file with a hex editor to view the column name (along with its hexa decimal equivalent) that contains a list of login names associated with the users.
29. Now, open **wordpress** folder, right-click **wp_users.frm** and select **Hex Edit with Hex Workshop v6.8** from the context menu.



30. We can observe that the login names are stored under the **user_login** column whose hexadecimal equivalent is **757365725F6C6F67696E**.

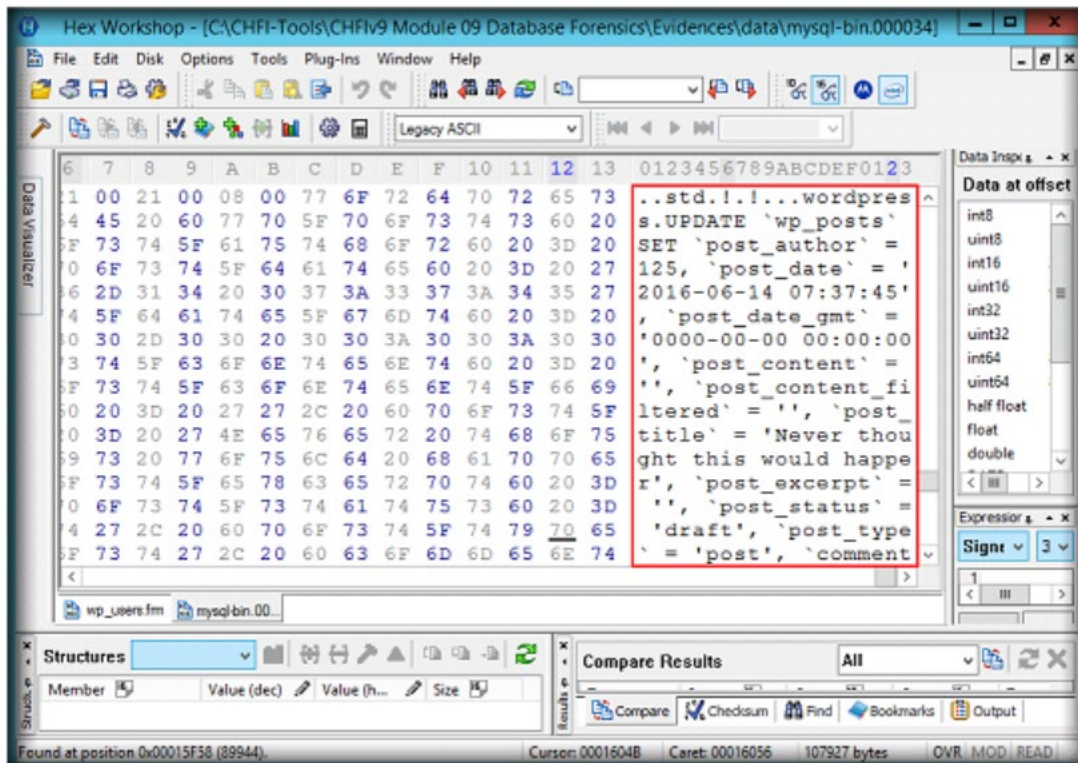


31. Using this phrase, we shall first find the attacker's login name, that is, **bad_guy** from the binary logs, and from there on, we shall trace the user activities performed by the malicious user.
32. In this lab, we shall analyze the **mysql-bin.000034** log file. Open the file with Hex Workshop.
33. Examine each binary log for the text string **user_login** or hex value **757365725F6C6F67696E**.

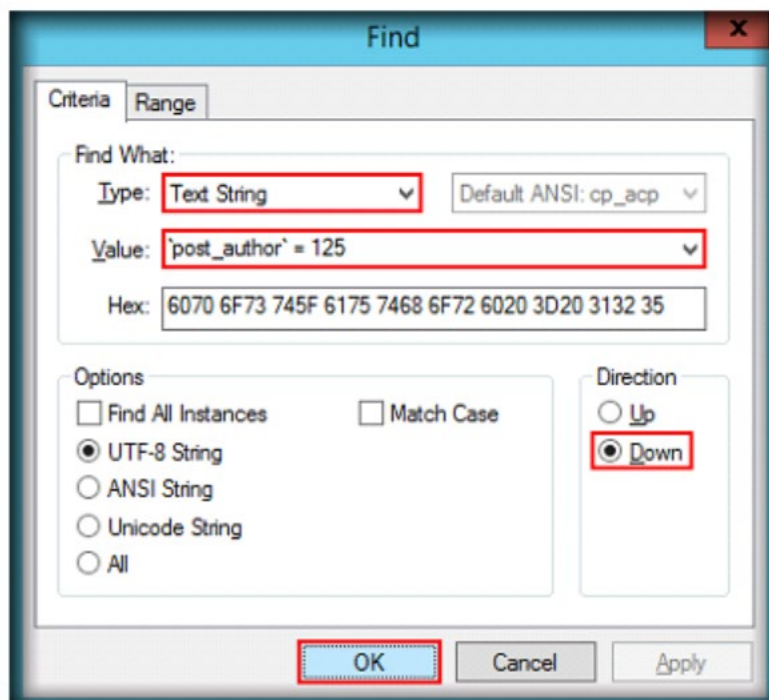


34. While conducting a detailed examination on the binary files, we can find that one of the binary files recorded an event where a query is executed for creating a user account with the
 - a. Login name – bad_guy
 - b. Password – pass123
 - c. Nice name – anonymous_hacker
 - d. Email ID – badguy@xyz.com

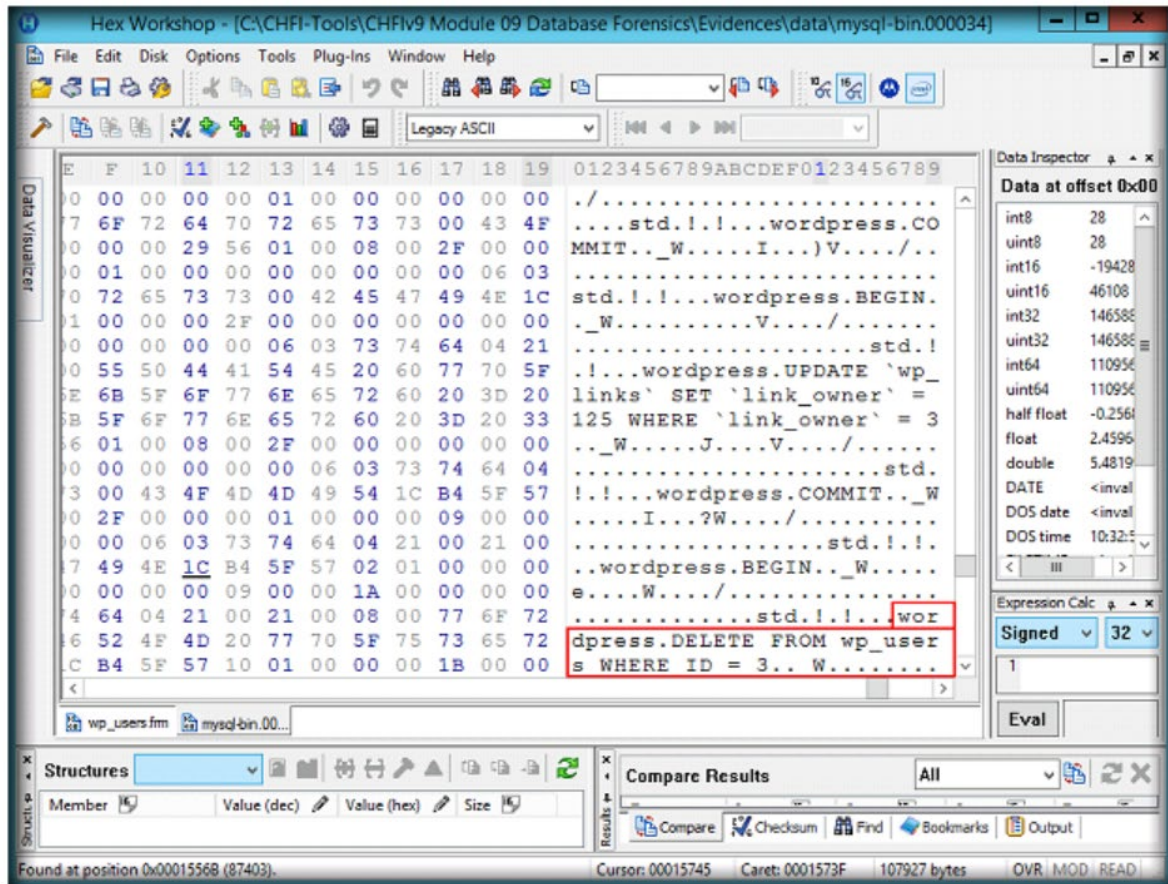
35. In the same way, scroll down the binary logs one-by-one to see the logs corresponding to the malicious user's actions.



36. We can observe that the attacker made a post (post_author id: 125) on 14th June, 2016 at GMT 07:37:45.
37. In the same way, you may search for all the actions performed by the attacker on the posts by looking for **'post_author' = 125** in the hex editor.
38. To find the actions performed by the attacker, press **Ctrl+F** on the keyboard. **Find** window appears. Select **Text String** from the **Type** drop-down list, enter **'post_author' = 125** in the **Value** text field, select **Down** radio-button under the **Direction** section and click **OK**.



39. While you scroll down the log file **mysql-bin.000034**, you will come across various actions performed on the database like user account deletion, new posts on the website, etc.



40. In the above screenshot, you can observe a **MySQL** query for deleting a user associated with the user ID 3. In the same way, you may examine all the log files and find the transactions performed by the attacker.

Lab Analysis

Analyze the results and document the findings of the lab.