Investigating Web Attacks

Module 08

Investigating Web Attacks

Web attacks are mainly intended to disrupt electronic commerce. Preventing cybercrime should be one of the top priorities for any organization. Investigating web attacks involves analyzing web server, FTP, and local system logs to confirm a web attack.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

An electronic commerce firm has been facing server issues due to continuous DDOS attacks from remote systems. The company hired an investigation team to look into the issue and find the perpetrator responsible for the web attack as well as to find the network or server vulnerabilities responsible for the attack.

In order to investigate the web attacks, as a **forensic investigator**, you must be able to analyze domain and IP address queries, and you must be thorough in the web security assessment protocols and in finding out vulnerabilities.

Lab Objectives

The objective of this lab is to provide expert knowledge that includes

- Analyzing domain and IP address queries

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 08 Investigating Web Attacks

Lab Environment

To carry out the lab objectives, you need the following:

- A computer running on **Windows Server 2012**
- A web browser with an **Internet** connection
- Administrative privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview of Web Attacks

There are different types of web attacks. For example, in a **denial-of-service (DoS) attack**, customers are **denied any access to information** or services available on the website. In such cases, customers report the unavailability of online services because the attacker prevents the legitimate user from **accessing websites**, **email accounts**, and other services that rely on the victim's computer.

Another indication of a web attack can be **redirecting of a web page** to an unknown website. When a user types the URL in the **address bar**, he or she is unable to access the site, and instead of accessing the intended site, the user is redirected to some other unknown site.

Unusual **slow network performance and frequent rebooting** of the server give indications of a web attack.

TASK 1

Overview

Lab Tasks

Recommended labs to assist you in investigating web attacks:

- Analyzing domain and IP address queries Using **SmartWhois** Tool

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab

1

Analyzing 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.

ICON KEY

🗀 Valuable information

✎ Test your knowledge

💻 Web exercise

📖 Workbook review

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.

🗀 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 08 Investigating Web Attacks**

Lab Environment

To carry out the lab, you need:

- **SmartWhois** tool, located at **C:\CHFI-Tools\CHFIv9 Module 08 Investigating Web Attacks\Tools for Locating IP Address\SmartWhois**.
- 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.

Lab Duration

Time: 15 Minutes

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?

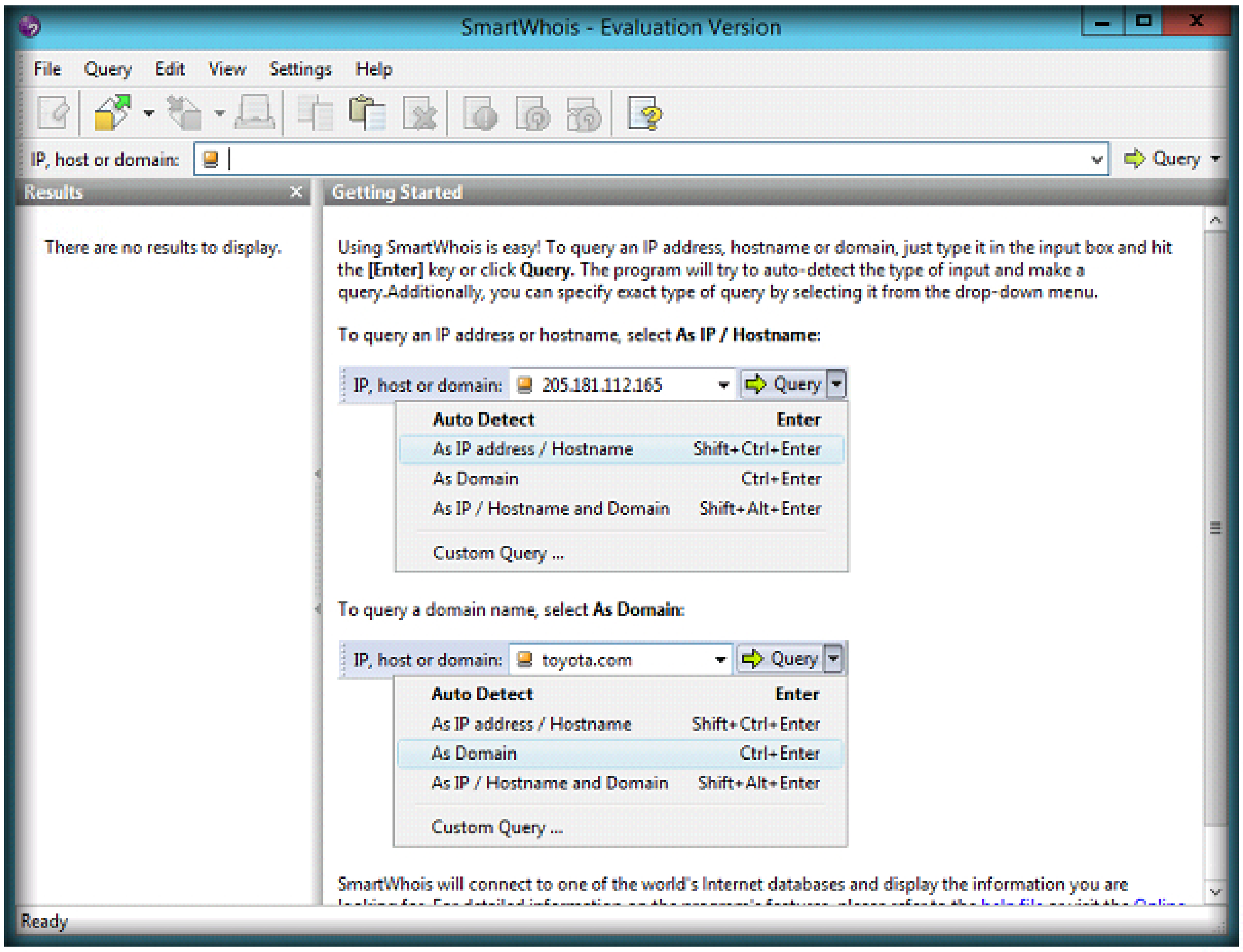
Lab Tasks

TASK 1

Launching SmartWhois

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 08 Investigating Web Attacks\Tools for Locating IP Address\SmartWhois**.
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.



There are no results to display.

Using SmartWhois is easy! To query an IP address, hostname or domain, just type it in the input box and hit the **[Enter]** key or click **Query**. The program will try to auto-detect the type of input and make a query.Additionally, you can specify exact type of query by selecting it from the drop-down menu.

To query an IP address or hostname, select **As IP / Hostname:**

IP, host or domain: 205.181.112.165

To query a domain name, select **As Domain:**

IP, host or domain: toyota.com

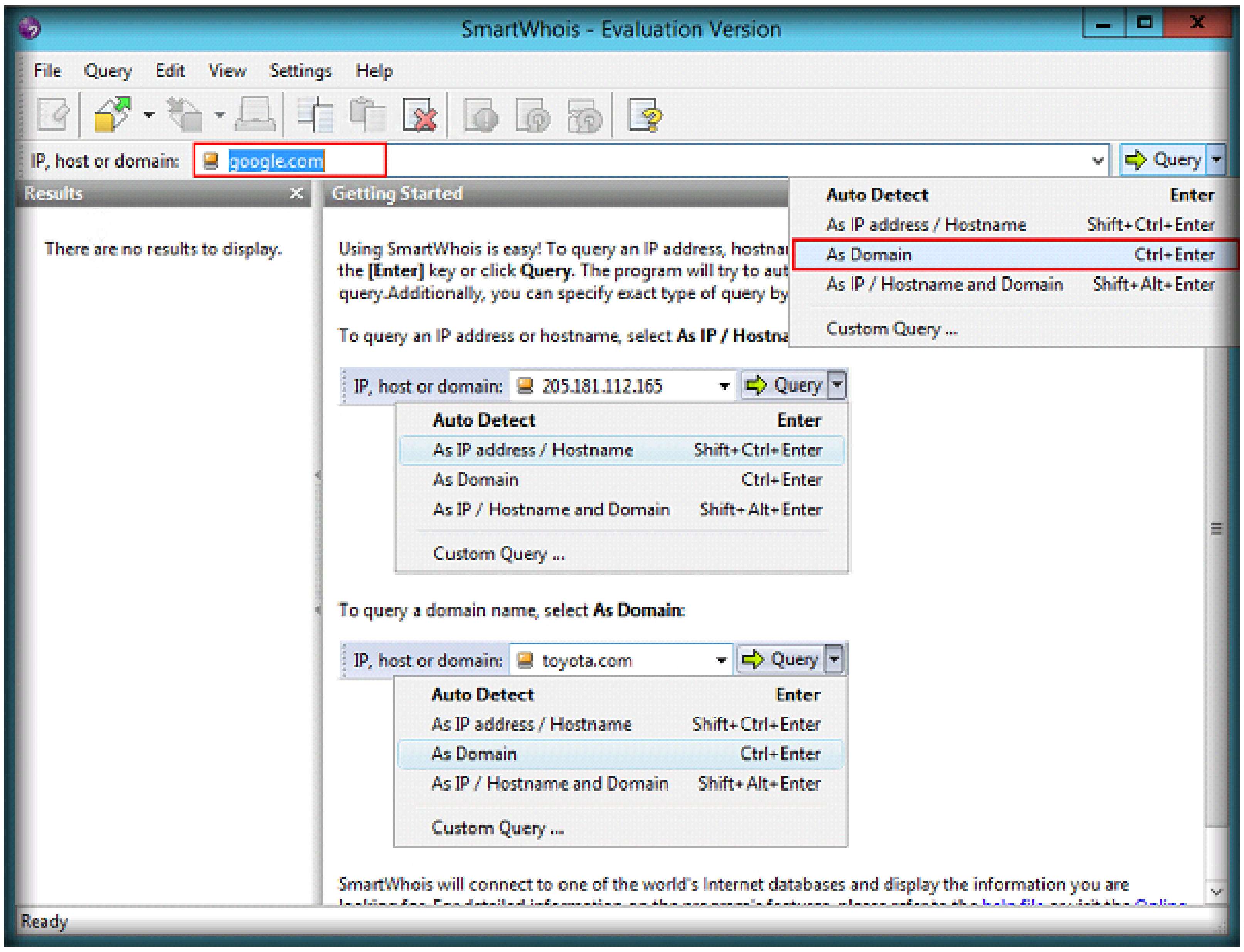
SmartWhois will connect to one of the world's Internet databases and display the information you are

FIGURE 1.1: The SmartWhois main window

TASK 2

Performing Domain Name Query

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.


SmartWhois - Evaluation Version
File
Query
Edit
View
Settings
Help
Query
Results
Getting Started
Auto Detect Enter
As IP address / Hostname Shift+Ctrl+Enter
As Domain Ctrl+Enter
As IP / Hostname and Domain Shift+Alt+Enter
Custom Query ...
Ready

IP, host or domain: google.com

There are no results to display.

Using SmartWhois is easy! To query an IP address, hostna the **[Enter]** key or click **Query**. The program will try to aut query.Additionally, you can specify exact type of query by

To query an IP address or hostname, select **As IP / Hostna**

IP, host or domain: 205.181.112.165

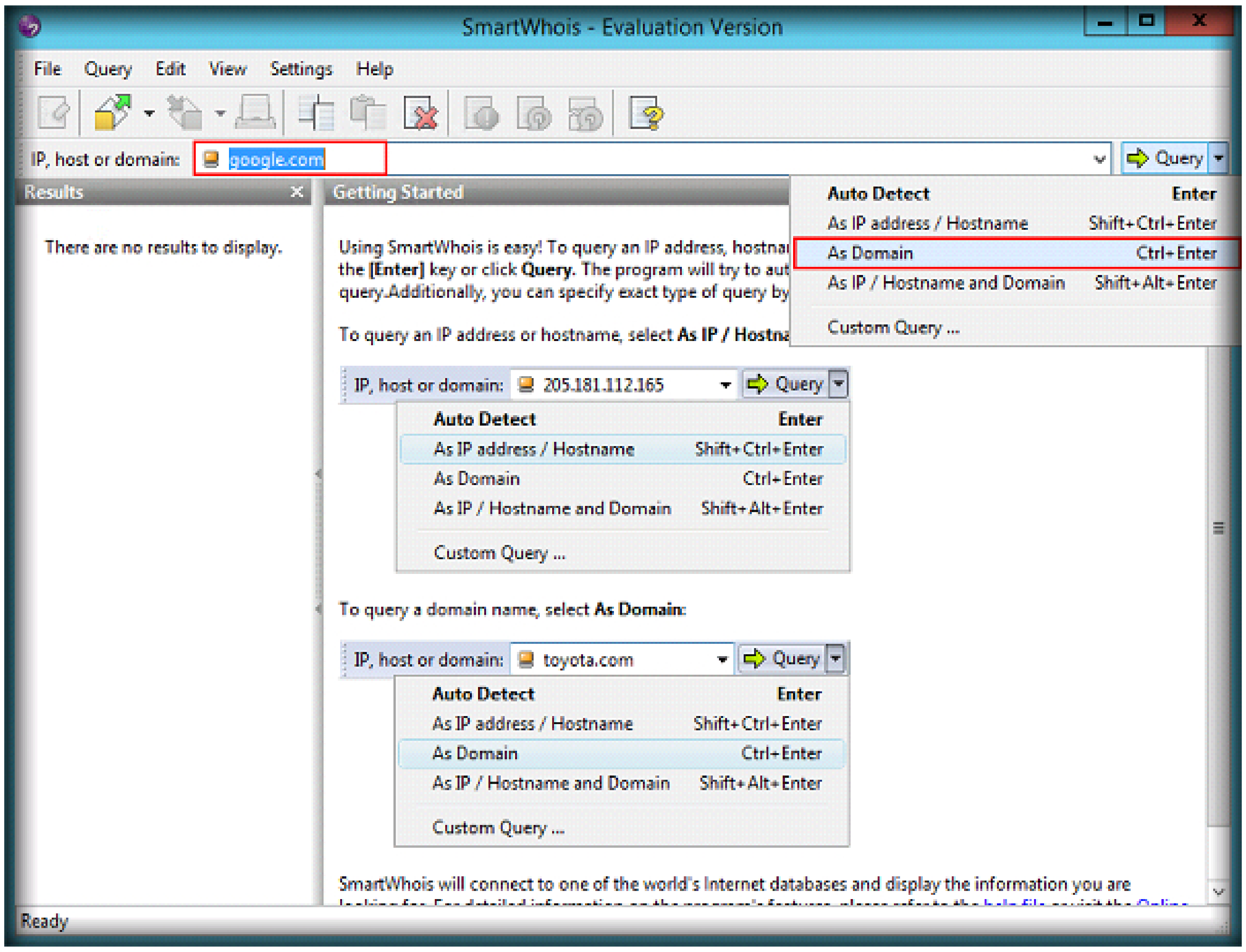
To query a domain name, select **As Domain**:

IP, host or domain: toyota.com

SmartWhois will connect to one of the world's Internet databases and display the information you are

FIGURE 1.2: SmartWhois domain name query

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


SmartWhois - Evaluation Version
File
Query
Edit
View
Settings
Help
Query
Results
Getting Started
Auto Detect Enter
As IP address / Hostname Shift+Ctrl+Enter
As Domain Ctrl+Enter
As IP / Hostname and Domain Shift+Alt+Enter
Custom Query ...
Ready

IP, host or domain: google.com

There are no results to display.

Using SmartWhois is easy! To query an IP address, hostna the **[Enter]** key or click **Query**. The program will try to aut query.Additionally, you can specify exact type of query by

To query an IP address or hostname, select **As IP / Hostna**

IP, host or domain: 205.181.112.165

To query a domain name, select **As Domain**:

IP, host or domain: toyota.com

SmartWhois will connect to one of the world's Internet databases and display the information you are

FIGURE 1.3: SmartWhois domain query results

Features:

Looks up whois data in the right database

Integration with Microsoft Internet Explorer and Microsoft Outlook

Saving results into an archive

Batch processing of IP addresses or domain lists

Caching of obtained results

Hostname resolution and DNS caching

Wildcard queries

Whois console for custom queries

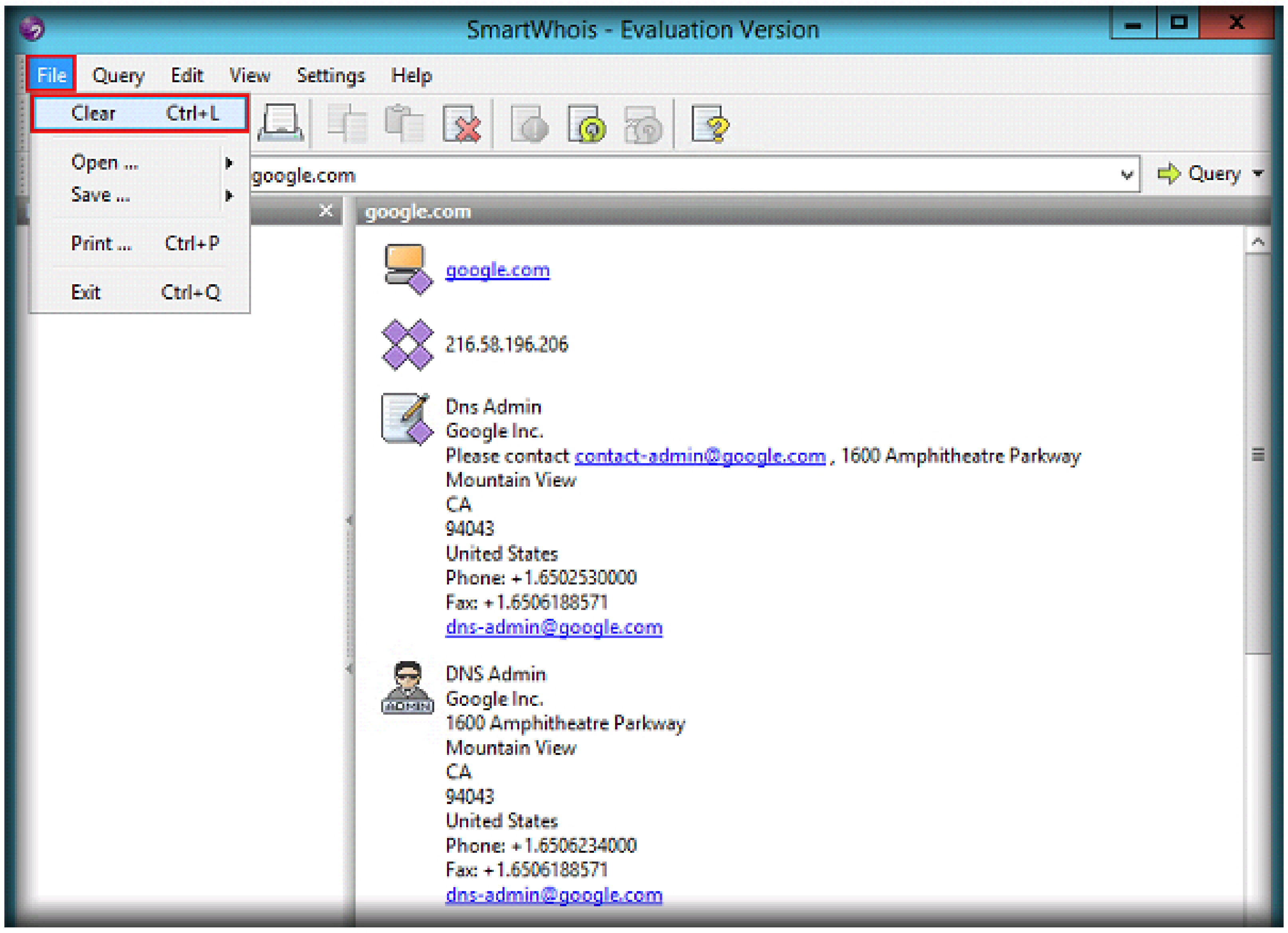
Country code reference

SOCKS5 firewall support

TASK 3

Clearing History

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



google.com

216.58.196.206

Dns Admin
Google Inc.
Please contact contact-admin@google.com , 1600 Amphitheatre Parkway
Mountain View
CA
94043
United States
Phone: +1.6502530000
Fax: +1.6506188571
dns-admin@google.com

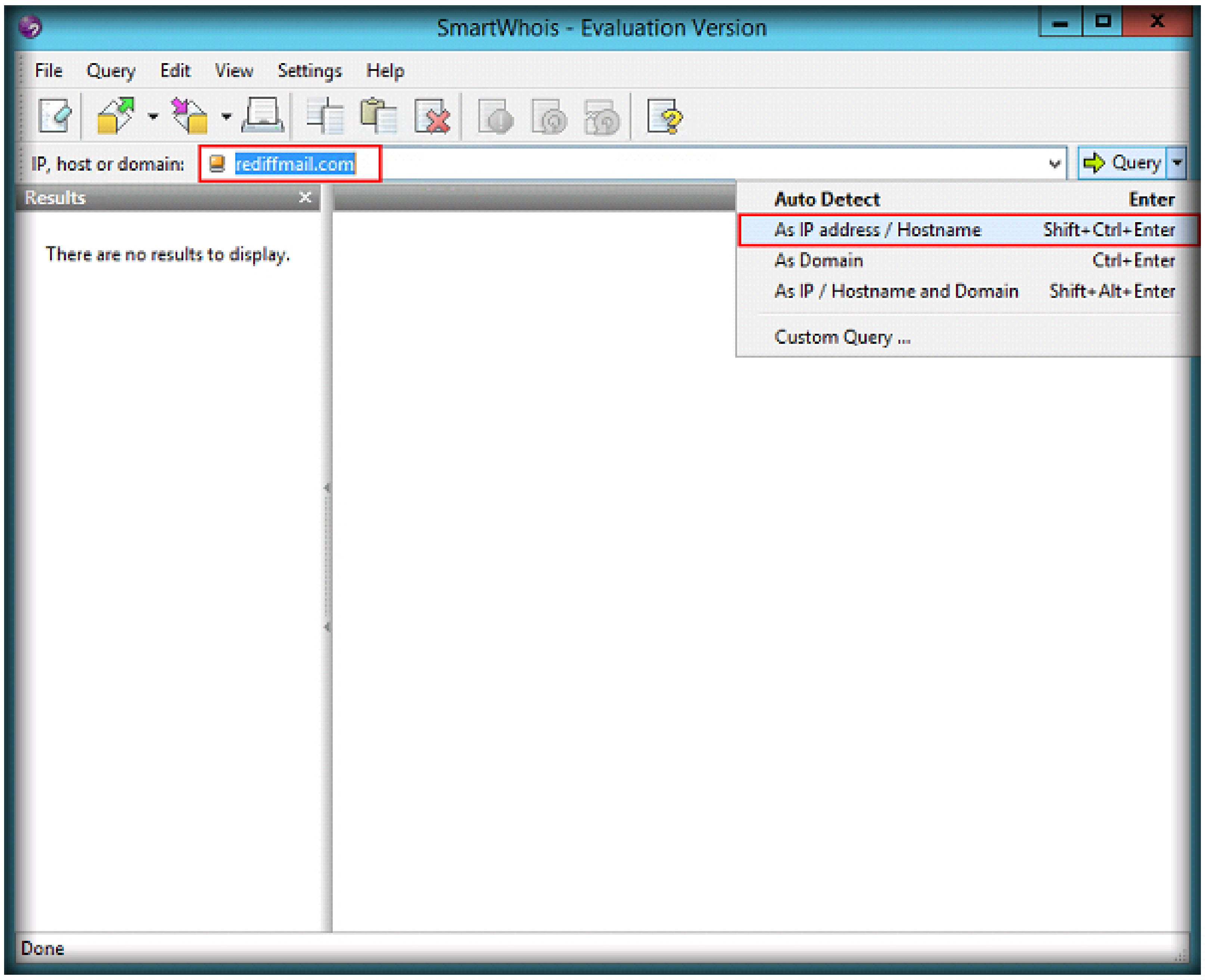
DNS Admin
Google Inc.
1600 Amphitheatre Parkway
Mountain View
CA
94043
United States
Phone: +1.6506234000
Fax: +1.6506188571
dns-admin@google.com

FIGURE 1.4: Clearing history

TASK 4

Performing Host Name Query

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.

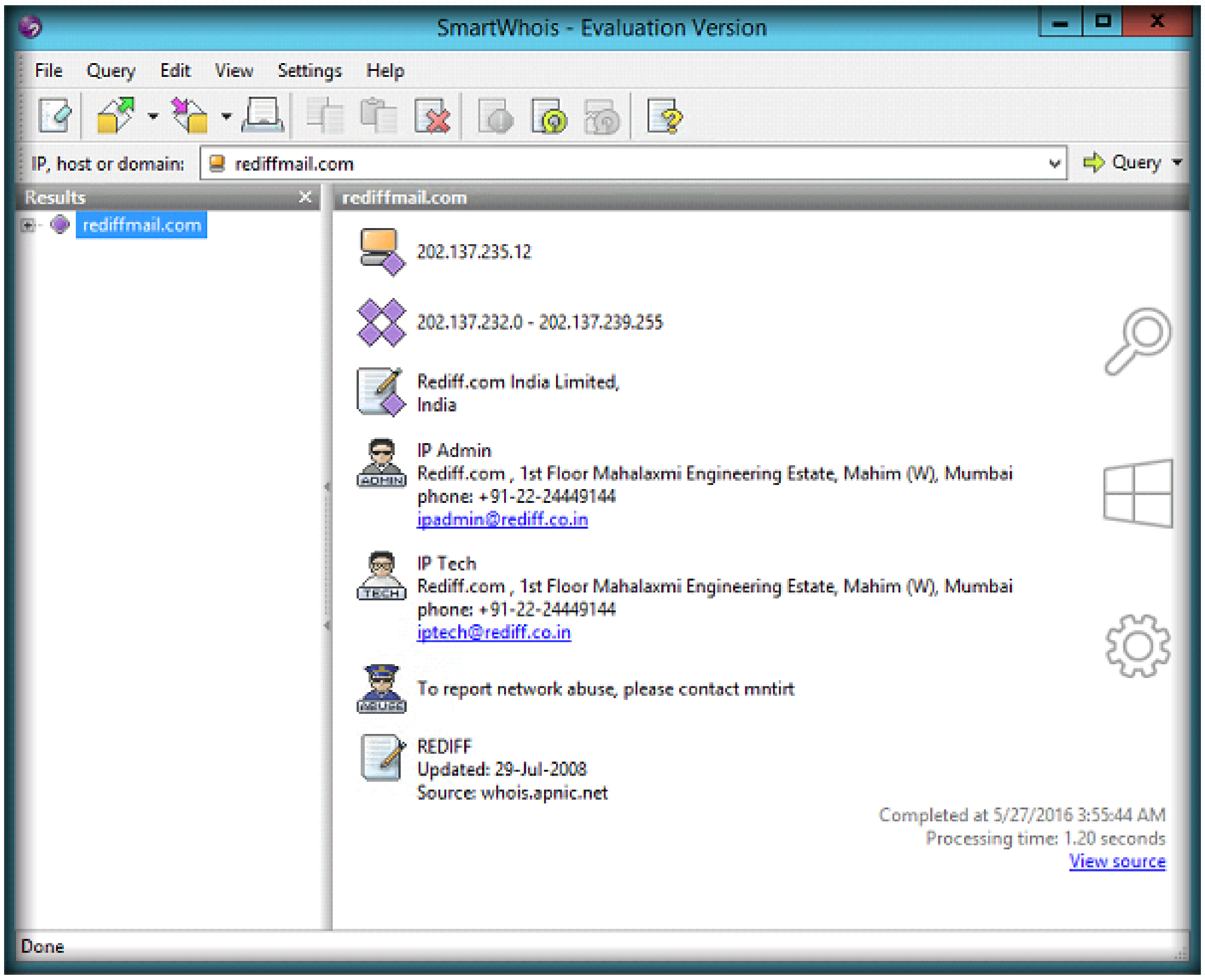

SmartWhois - Evaluation Version
File
Query
Edit
View
Settings
Help
Query
Results
Auto Detect Enter
As IP address / Hostname Shift+Ctrl+Enter
As Domain Ctrl+Enter
As IP / Hostname and Domain Shift+Alt+Enter
Custom Query ...
Done

IP, host or domain: rediffmail.com

There are no results to display.

FIGURE 1.5: SmartWhois hostname query

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


SmartWhois - Evaluation Version
File Query Edit View Settings Help
IP, host or domain:
Query
Results
Done

IP, host or domain: rediffmail.com

Results: rediffmail.com

```
202.137.235.12

202.137.232.0 - 202.137.239.255

Rediff.com India Limited,
India

IP Admin
Rediff.com , 1st Floor Mahalaxmi Engineering Estate, Mahim (W), Mumbai
phone: +91-22-24449144
ipadmin@rediff.co.in

IP Tech
Rediff.com , 1st Floor Mahalaxmi Engineering Estate, Mahim (W), Mumbai
phone: +91-22-24449144
iptech@rediff.co.in

To report network abuse, please contact mntirt

REDIFF
Updated: 29-Jul-2008
Source: whois.apnic.net

                                   Completed at 5/27/2016 3:55:44 AM
                                       Processing time: 1.20 seconds
                                                         View source
```

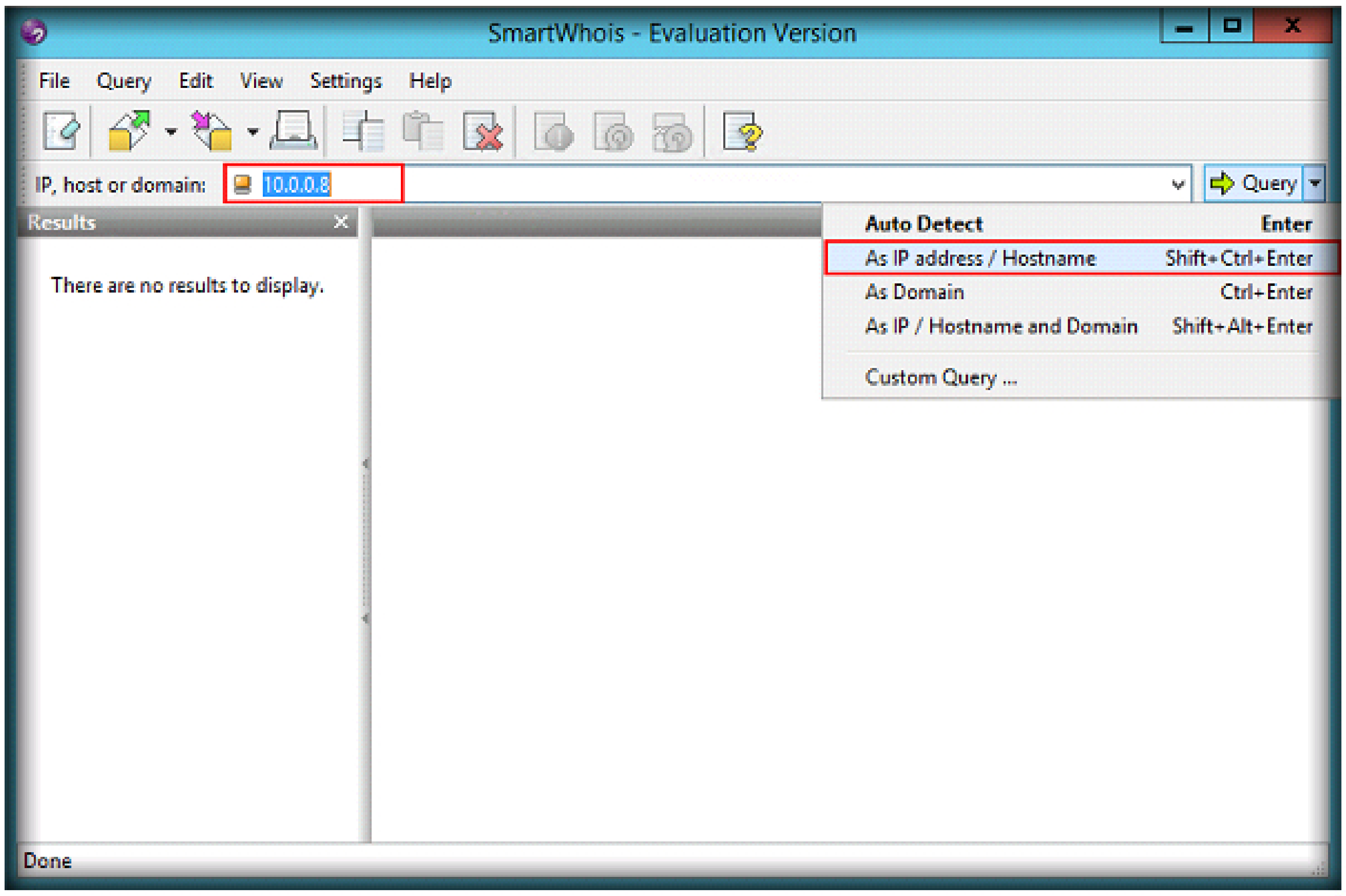
FIGURE 1.6: SmartWhois hostname query results

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

TASK 5

Performing IP Address Query

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.

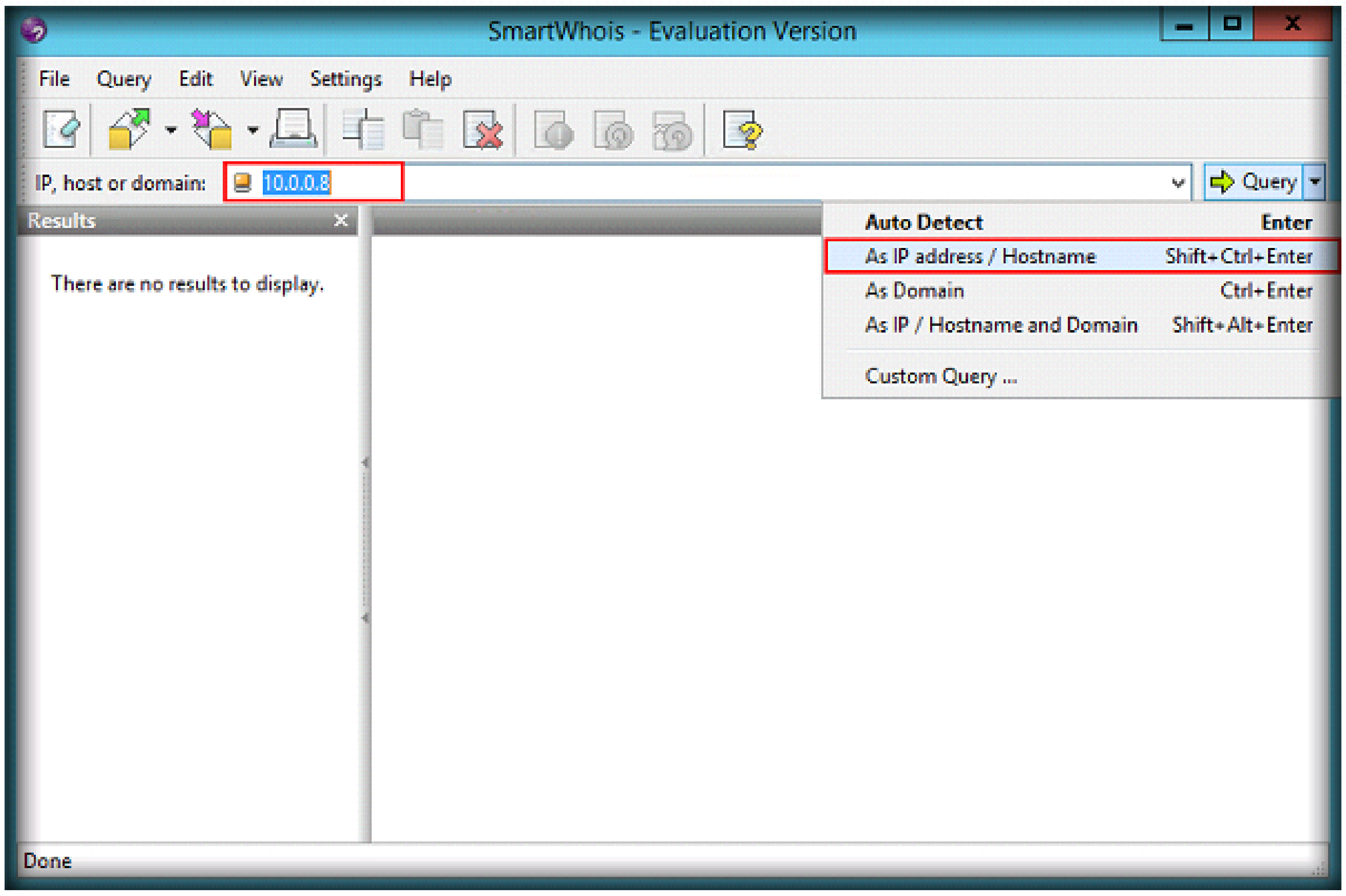

SmartWhois - Evaluation Version
File Query Edit View Settings Help
IP, host or domain:
Query
Results
Auto Detect Enter
As IP address / Hostname Shift+Ctrl+Enter
As Domain Ctrl+Enter
As IP / Hostname and Domain Shift+Alt+Enter
Custom Query ...
Done

IP, host or domain: 10.0.0.8

There are no results to display.

FIGURE 1.7: SmartWhois IP address query

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


SmartWhois - Evaluation Version
File Query Edit View Settings Help
Query
Results
Auto Detect Enter
As IP address / Hostname Shift+Ctrl+Enter
As Domain Ctrl+Enter
As IP / Hostname and Domain Shift+Alt+Enter
Custom Query ...
Done

IP, host or domain: 10.0.0.8

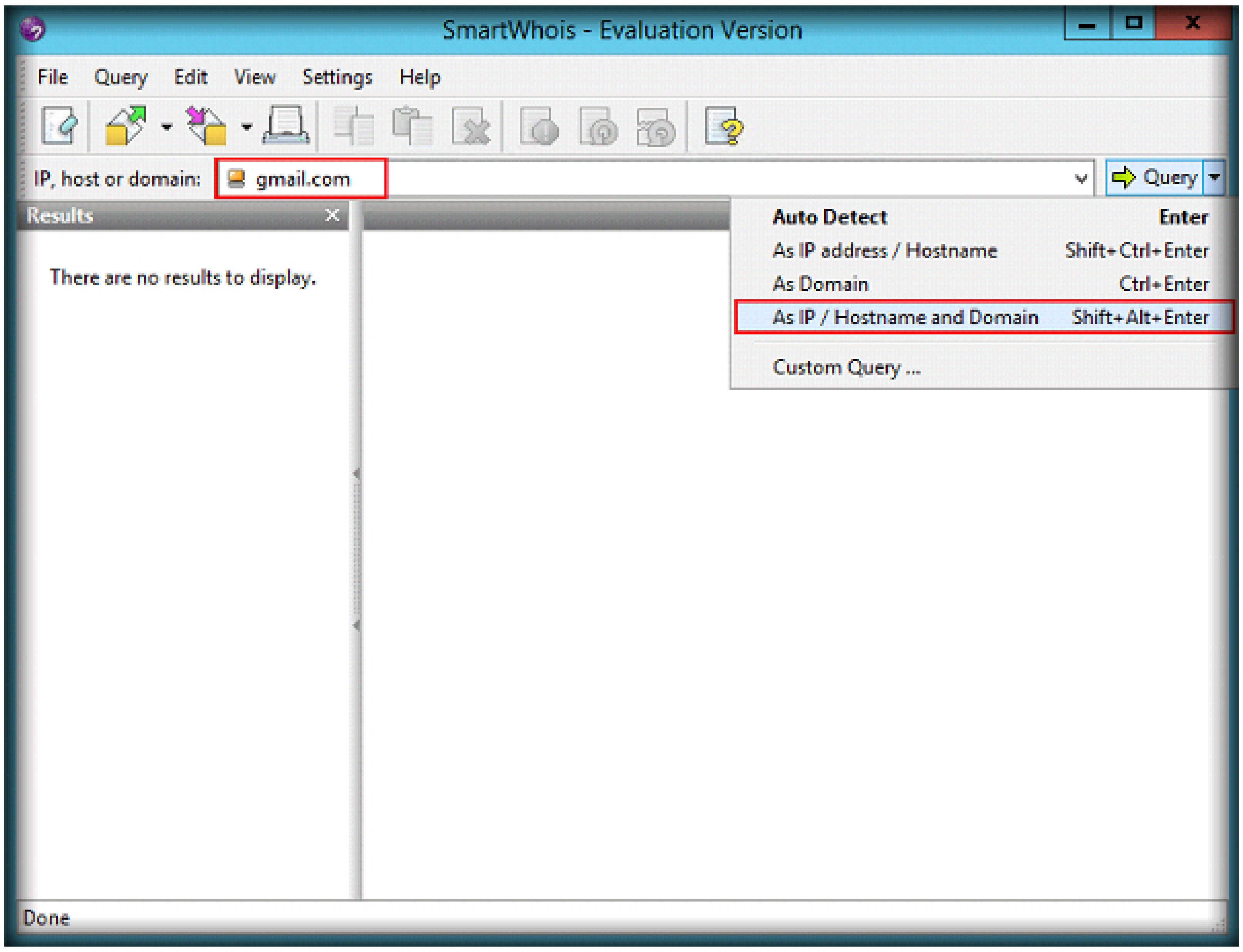
There are no results to display.

FIGURE 1.8: SmartWhois IP address query results

TASK 6

Performing IP/Hostname and Domain Query

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.

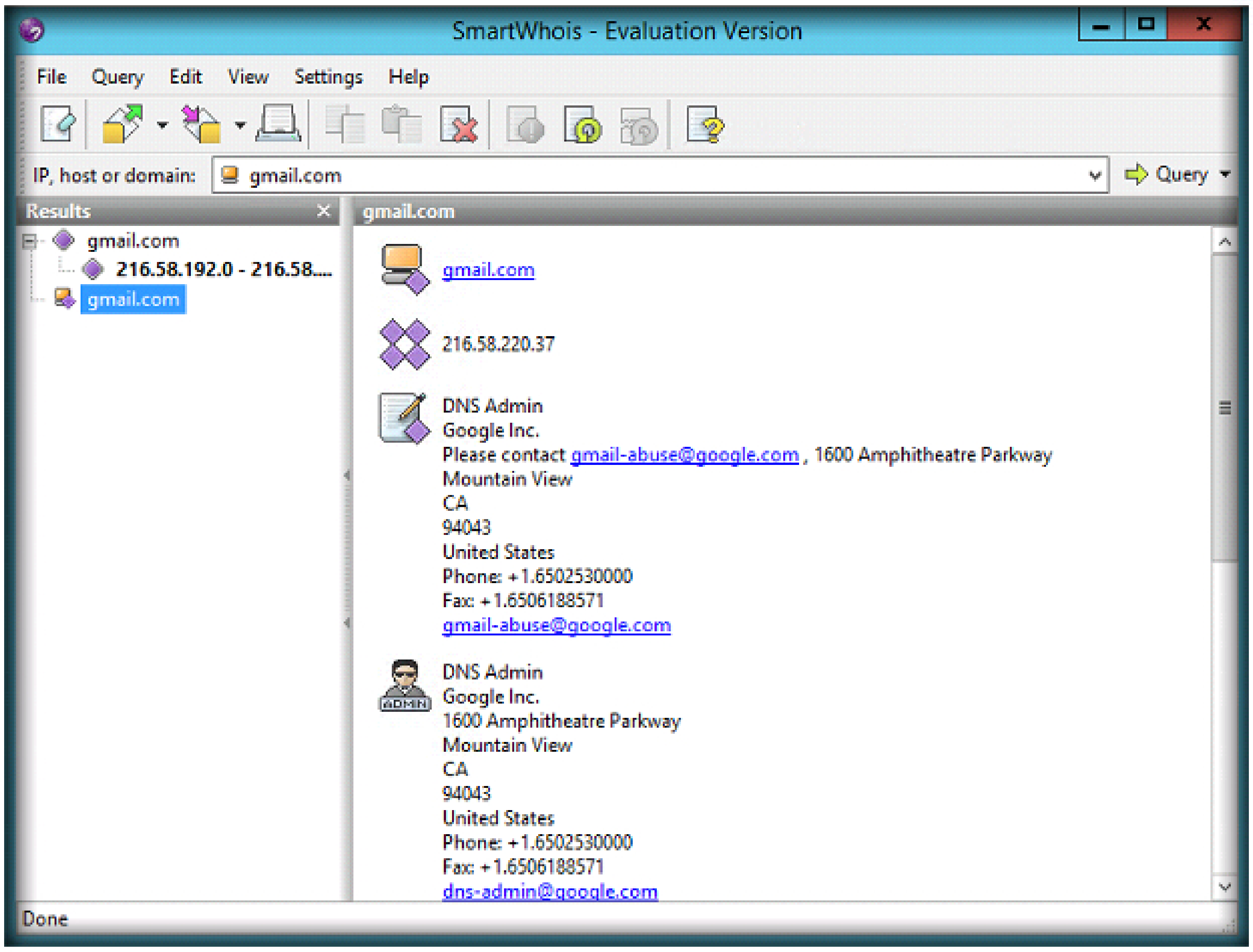

SmartWhois - Evaluation Version
File Query Edit View Settings Help
Query
Results
Auto Detect Enter
As IP address / Hostname Shift+Ctrl+Enter
As Domain Ctrl+Enter
As IP / Hostname and Domain Shift+Alt+Enter
Custom Query ...
Done

IP, host or domain: gmail.com

There are no results to display.

FIGURE 1.9: SmartWhois IP/hostname and domain 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.


SmartWhois - Evaluation Version
File Query Edit View Settings Help
IP, host or domain:
Query
Results
Done

IP, host or domain: gmail.com

Results:
- gmail.com
  - 216.58.192.0 - 216.58....
- gmail.com

gmail.com

gmail.com

216.58.220.37

DNS Admin
Google Inc.
Please contact gmail-abuse@google.com , 1600 Amphitheatre Parkway
Mountain View
CA
94043
United States
Phone: +1.6502530000
Fax: +1.6506188571
gmail-abuse@google.com

DNS Admin
Google Inc.
1600 Amphitheatre Parkway
Mountain View
CA
94043
United States
Phone: +1.6502530000
Fax: +1.6506188571
dns-admin@google.com

FIGURE 1.10: SmartWhois IP/hostname and domain query results

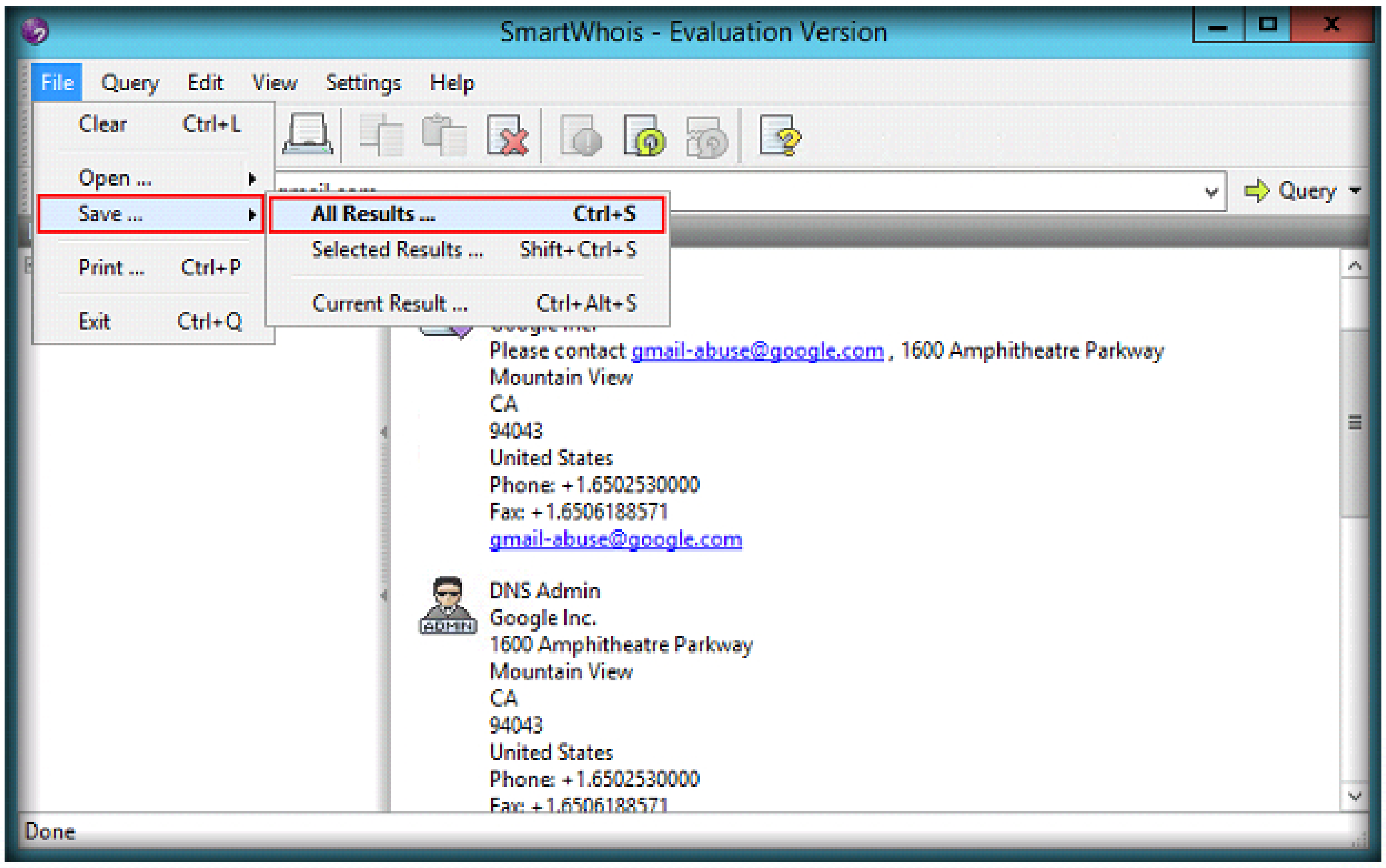
SmartWhois is integrated with CommView Network Monitor.

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

TASK 7

Saving the Results

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.

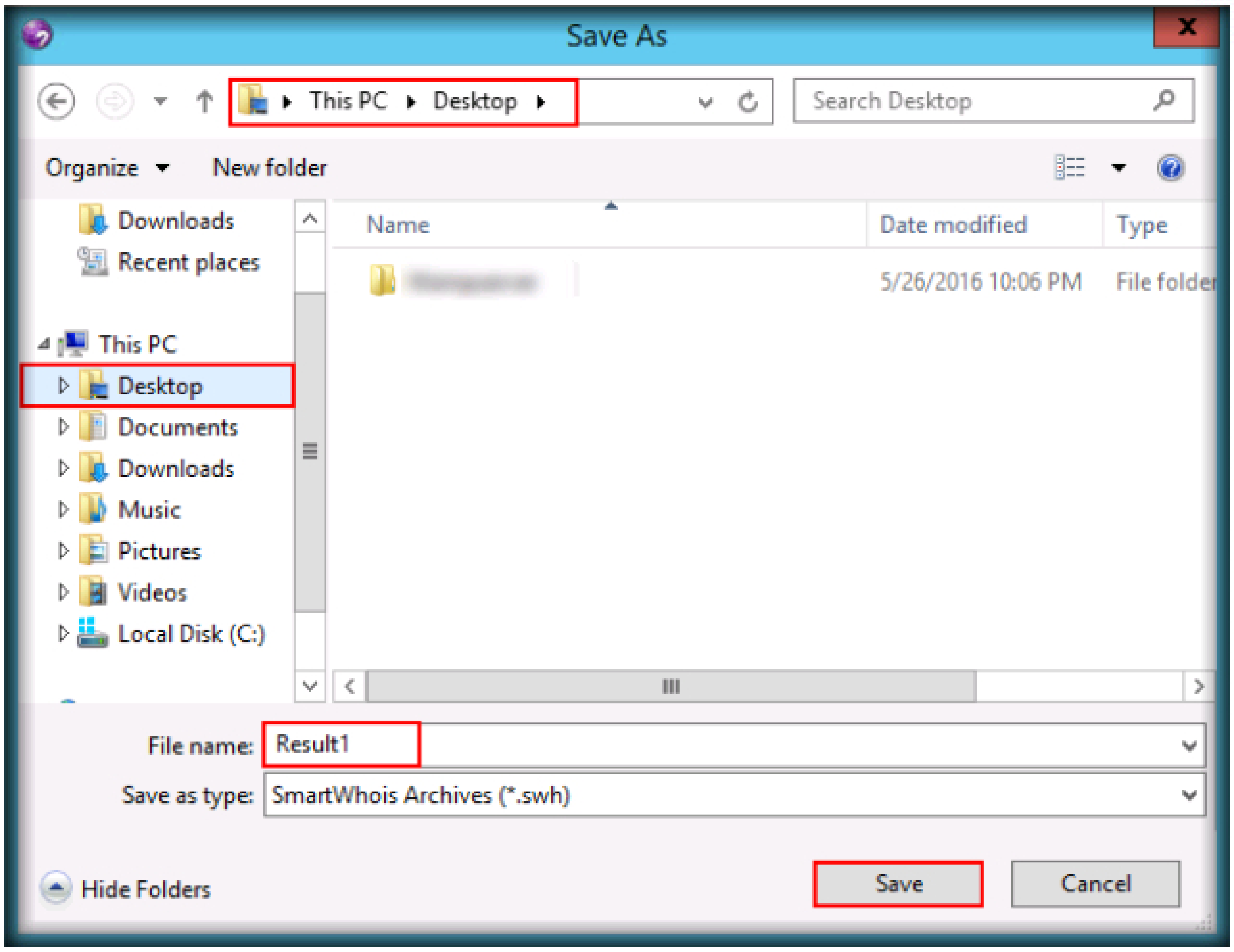

SmartWhois - Evaluation Version
File Query Edit View Settings Help
Clear Ctrl+L
Open ...
Save ...
Print ... Ctrl+P
Exit Ctrl+Q
All Results ... Ctrl+S
Selected Results ... Shift+Ctrl+S
Current Result ... Ctrl+Alt+S
Query
Done

Please contact gmail-abuse@google.com , 1600 Amphitheatre Parkway
Mountain View
CA
94043
United States
Phone: +1.6502530000
Fax: +1.6506188571
gmail-abuse@google.com

DNS Admin
Google Inc.
1600 Amphitheatre Parkway
Mountain View
CA
94043
United States
Phone: +1.6502530000
Fax: +1.6506188571

FIGURE 1.11: Saving results

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.)



File name: Result1

Save as type: SmartWhois Archives (*.swh)

FIGURE 1.12: SmartWhois Save As window

TASK 8

Opening the Saved Results Document

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

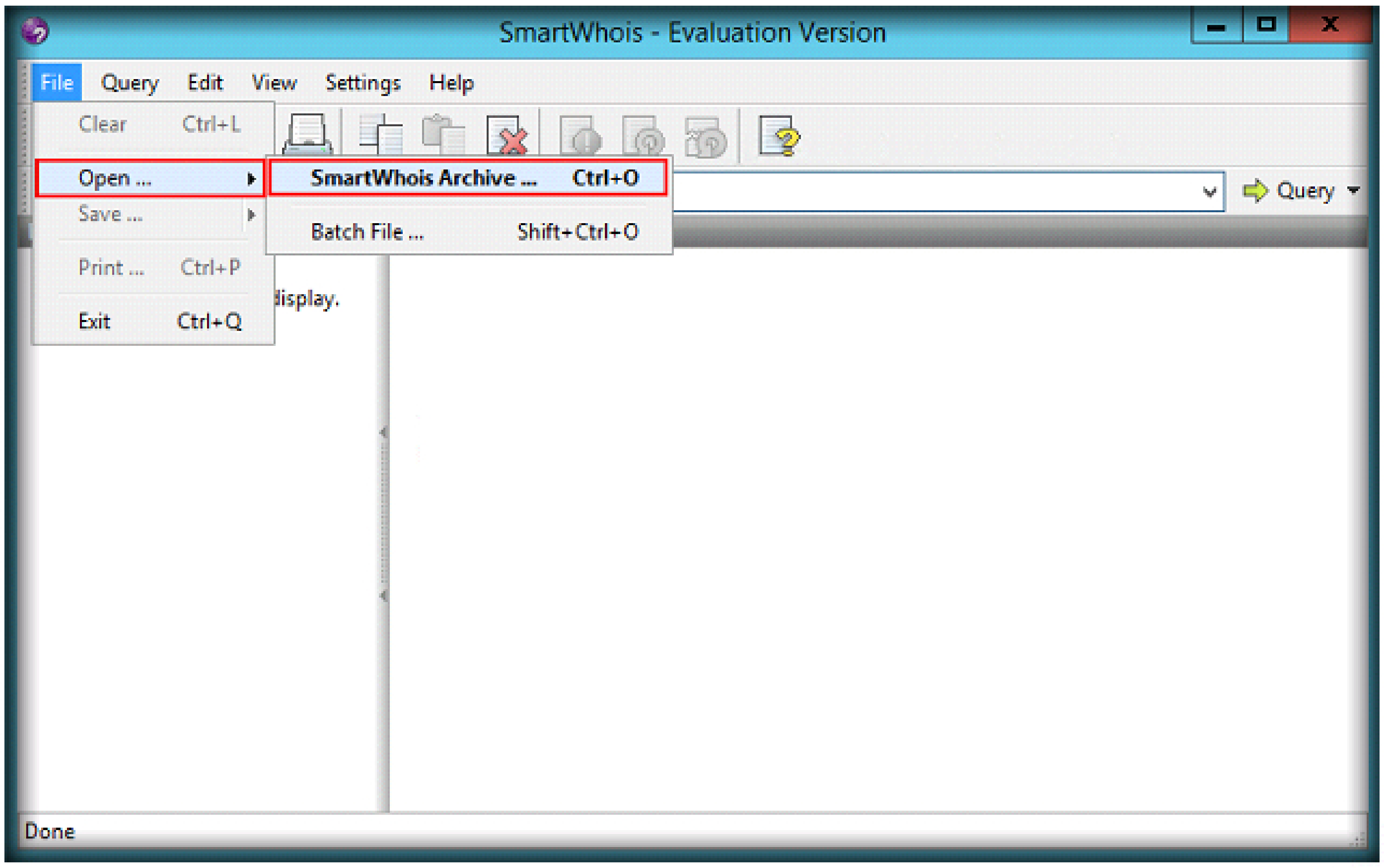
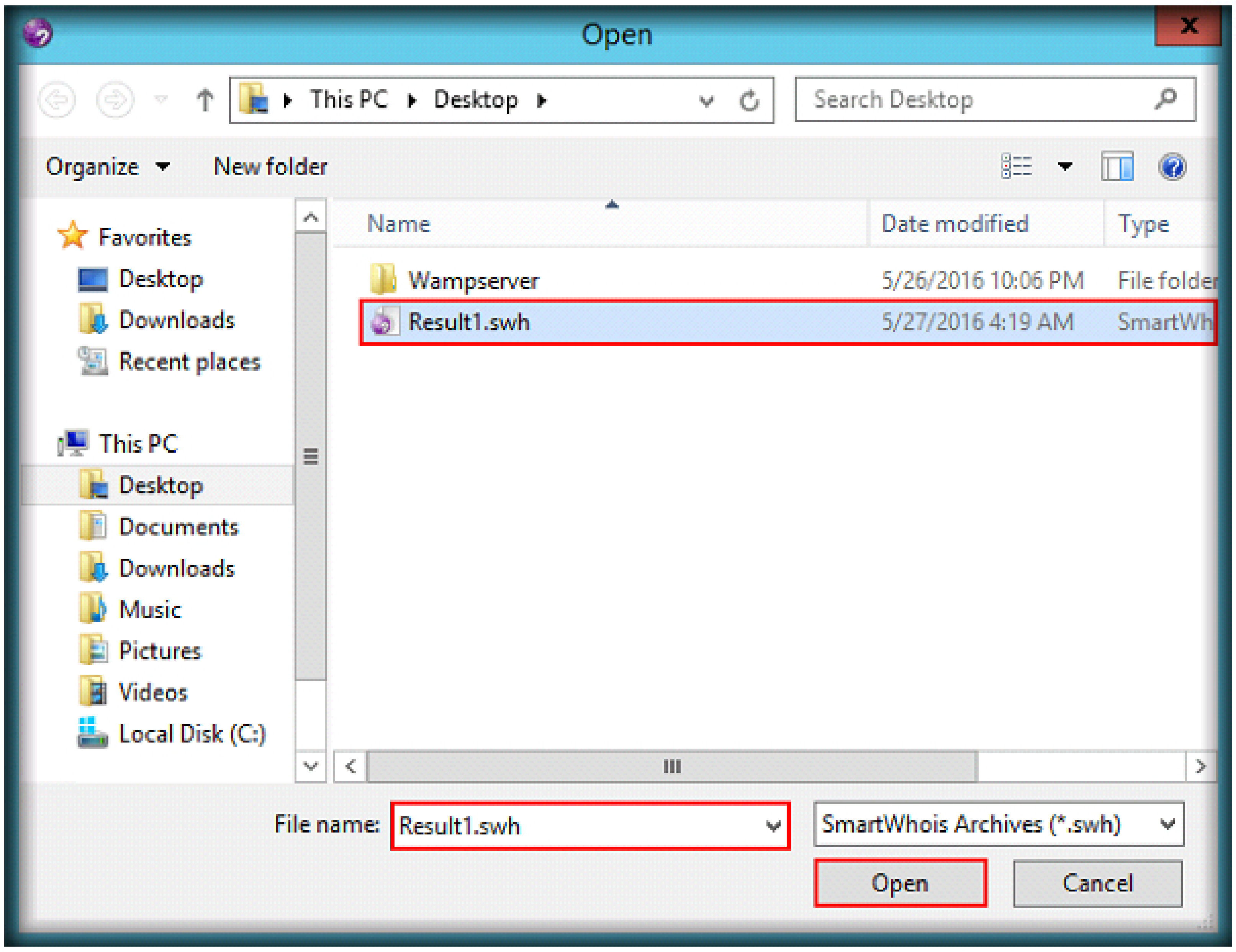


FIGURE 1.13: SmartWhois file menu

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



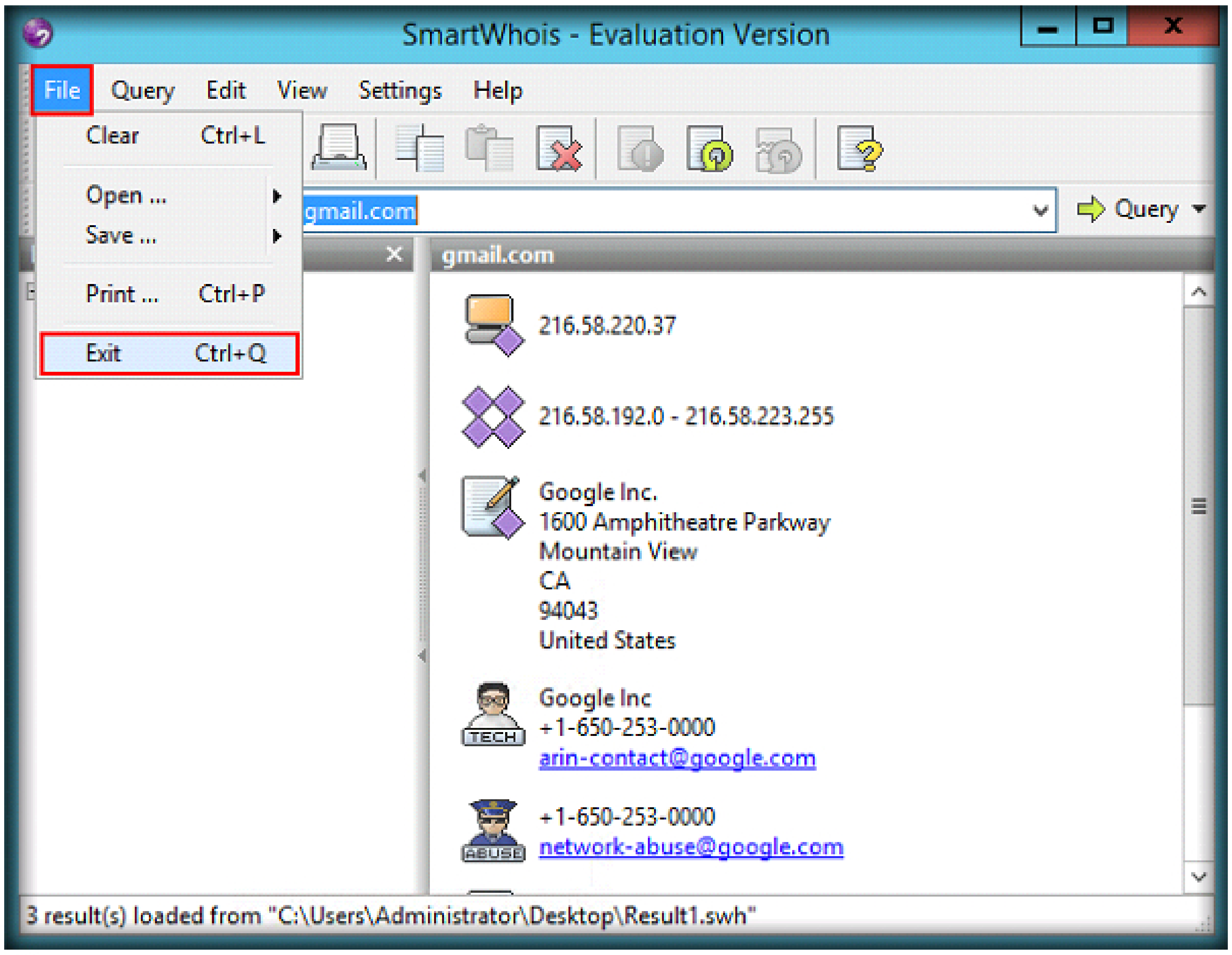
Name	Date modified	Type
Wampserver	5/26/2016 10:06 PM	File folder
Result1.swh	5/27/2016 4:19 AM	SmartWh

File name: Result1.swh

SmartWhois Archives (*.swh)

FIGURE 1.14: SmartWhois file open window

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



gmail.com

gmail.com

216.58.220.37

216.58.192.0 - 216.58.223.255

Google Inc.
1600 Amphitheatre Parkway
Mountain View
CA
94043
United States

Google Inc
+1-650-253-0000
arin-contact@google.com

+1-650-253-0000
network-abuse@google.com

3 result(s) loaded from "C:\Users\Administrator\Desktop\Result1.swh"

FIGURE 1.15: SmartWhois Exit

Lab Analysis

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

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs