



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



Advanced Cyber Security (ACS)

Lab – Footprinting & Reconnaissance
and
Scanning Networks

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

Task 1: Footprinting & Reconnaissance - Collecting Information about a Target by Tracing Emails

Footprinting refers to collecting as much information as possible regarding a target network from publicly accessible sources.

Tracing emails involves analyzing the email header to discover details about the sender.

Lab Scenario

An attacker may send malicious emails to a victim (employee) in order to carry out an attack on a target organization. As a professional ethical hacker, you should be able to trace out information about such malicious email. It involves analyzing the email headers or suspicious email to extract information such as the date that an email was received or opened, geographical information, etc.

Lab Objectives

The objective of this lab is to demonstrate email tracing using eMailTrackerPro.

Pre- Activity exercise

To carry out the lab, you need:

1. Install Windows 7 or Windows 10 in Virtual Box which is on the shared drive as instructed by your tutor.
2. The eMailTrackerPro is also on the Shared OneDrive, https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvI2SguS-JxOkvHyQJGUXdUB5ZbwqVWk3IHGxl2zndTtw?e=EwEBQ7
3. You can also download the latest version of eMailTrackerPro from this link from <http://www.emailtrackerpro.com/download.html>
4. The latest emailtrackerpro may be a trial version and in some instance may have a name change.
5. Note the screenshot in this lab might differ slightly.
6. Administrative privileges required.
7. A valid email account (Hotmail, Gmail, yahoo, etc.). We suggest you to signup with any of these services to obtain a new email account for this lab. ***Do not use your real email account and password in this exercise.***

Overview of Email Tracing/Tracking

E-mail tracking is a method to monitor or spy on email delivered to the intended recipient. It reveals information such as:

- When an email message was received and read
- If destructive email was sent
- The GPS coordinates and map location of the recipient
- The time spent reading the email
- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time.

Activity:

1. Logon to the virtual machine
2. Navigate to the shared OneDrive folder to https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EvI2SguS-JxOkvHyQJGUXdUB5ZbwqVWk3IHGxI2zndTtw?e=EwEBQ7 for eMailTrackerPro and double click emt.exe
3. If the **Open File – Security Policy** pop-up appears, click Run
4. Follow the wizard steps (be selecting default options) to install eMailTrackerPro.
5. In the last step of installation, unchecked Show Readme option and click finishe. If the application does not launce automatically, then Launch the eMailTrackerPro from the start menu.

6. The main window of eMailTrackerPro appears along with the **Edition Selection** pop-up. Click **OK**.

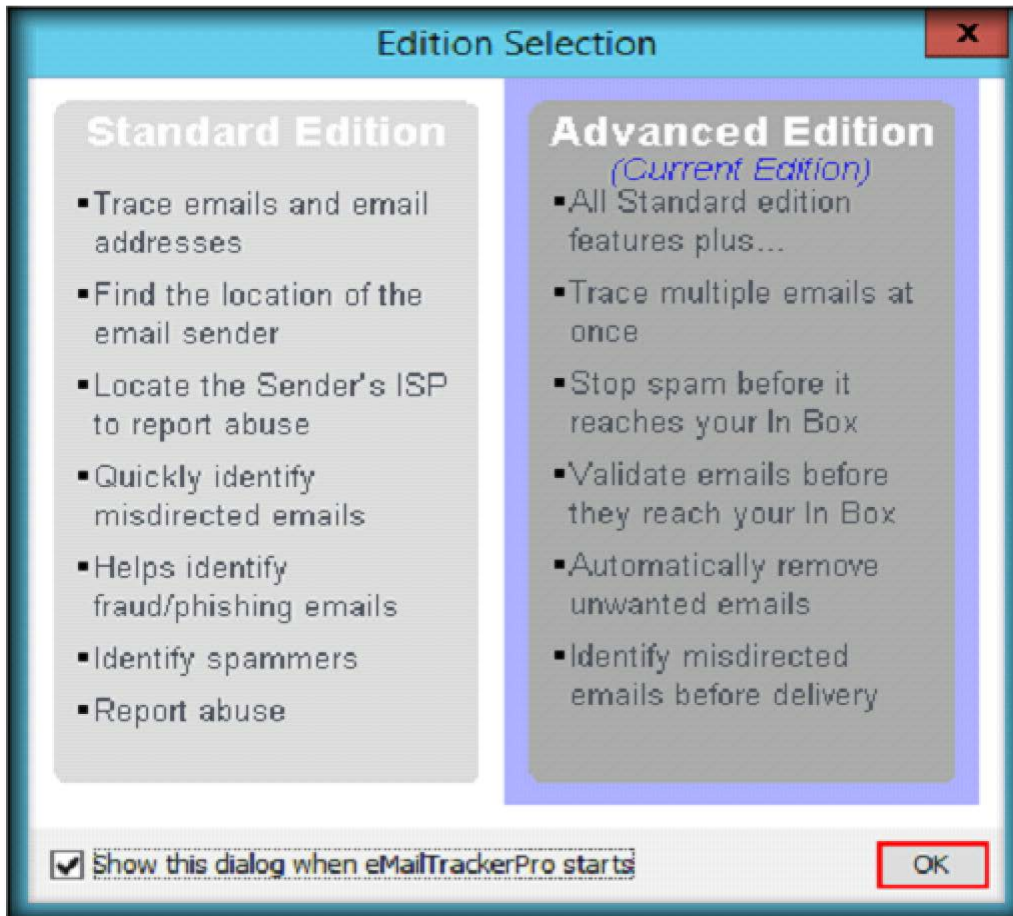


FIGURE 6.1: eMailTrackerPro edition Selection pop-up window

7. The **eMailTrackerPro** main window appears as shown in the following screenshot:

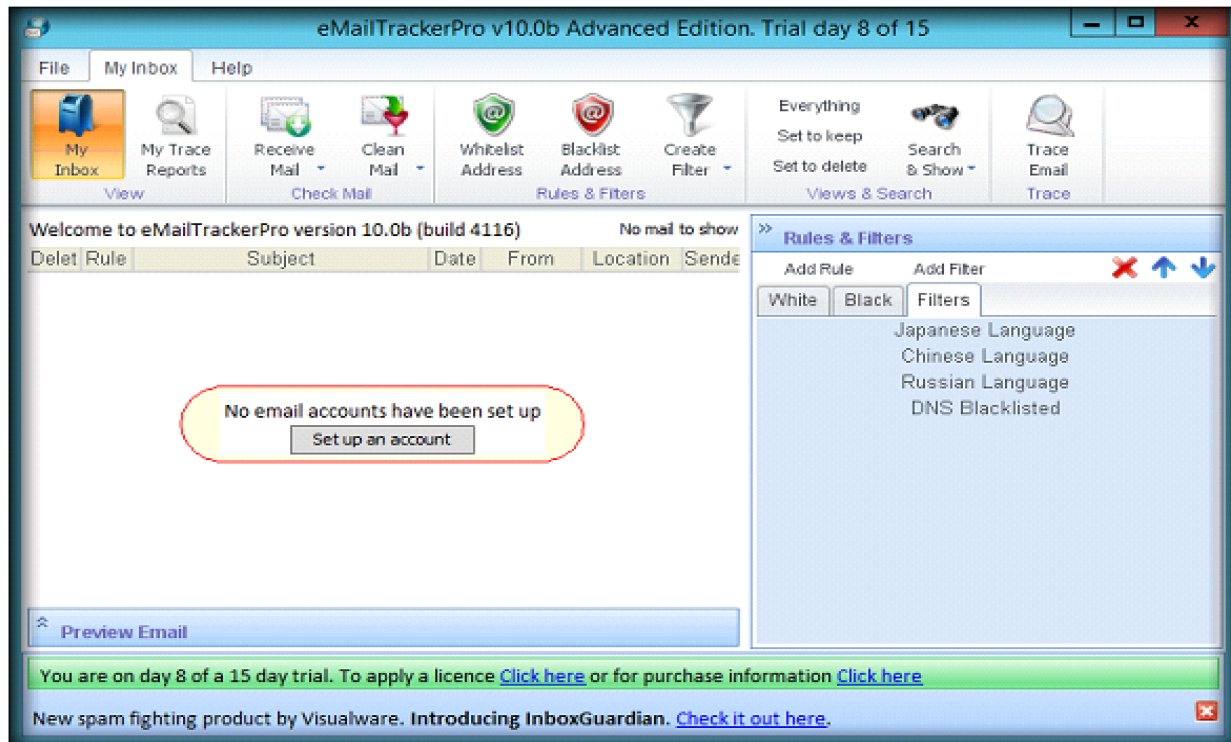


FIGURE 6.2: eMailTrackerPro main window

8. Click **My Trace Reports**.

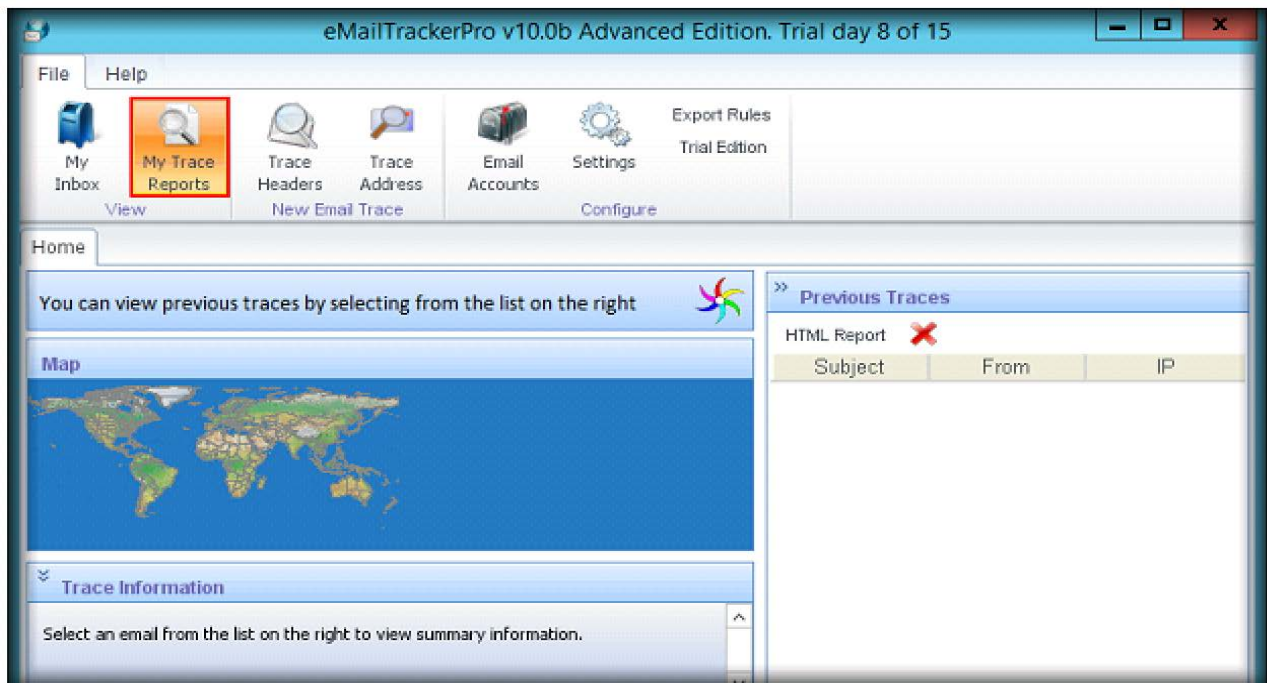


FIGURE 6.3: The eMailTrackerPro Main window

9. Click **Trace Headers** to start the trace.
10. Select **Trace an email I have received**. Copy the email header from the email you wish to trace and paste it in the **Email headers** field under **Enter Details**.

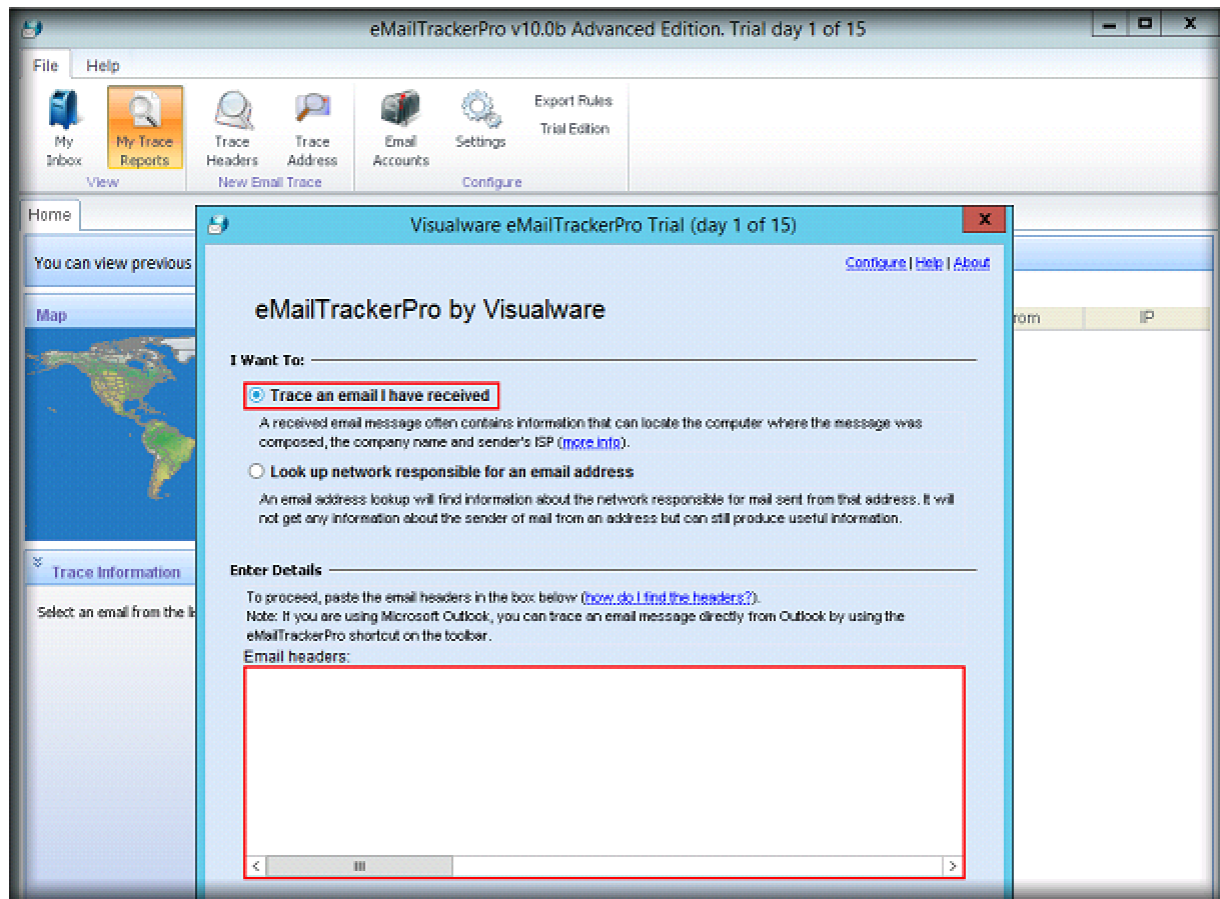


FIGURE 6.4: The eMailTrackerPro entering details window

11. Log in to an email account and open the message you'd like to view headers for.
12. Click the down arrow next to **Reply**, at the top of the message pane.
13. Select **Show Original** from the drop-down list.

Note: In Outlook, find the email header by following the steps below:

- Double-click the email to open it in a new window.
- Click the small arrow in the lower right corner of the **Tags** toolbar box to open **Message Options** information box.
- Under **Internet headers**, you will find the **Email header**.

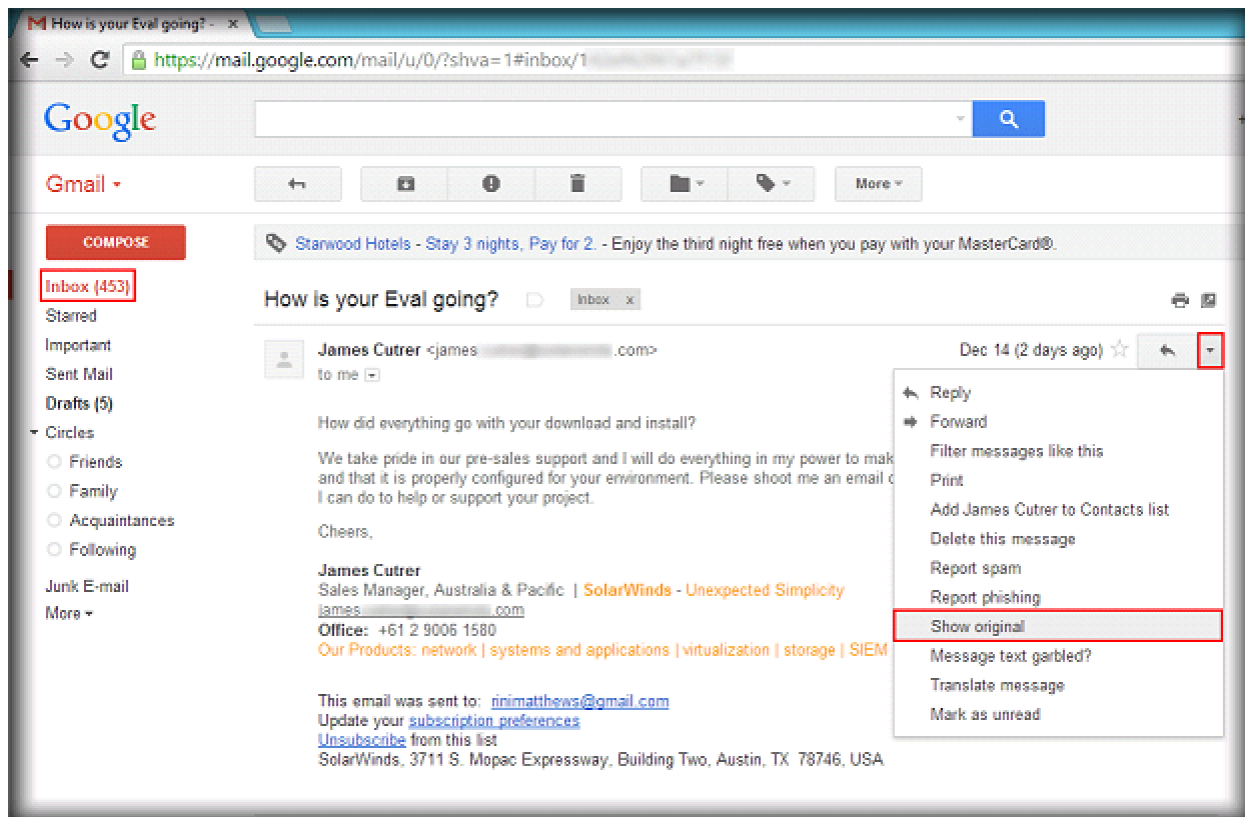


FIGURE 6.5: Finding Email Header in Outlook 2010

14. The header appears in a new tab as shown in the following screenshot:

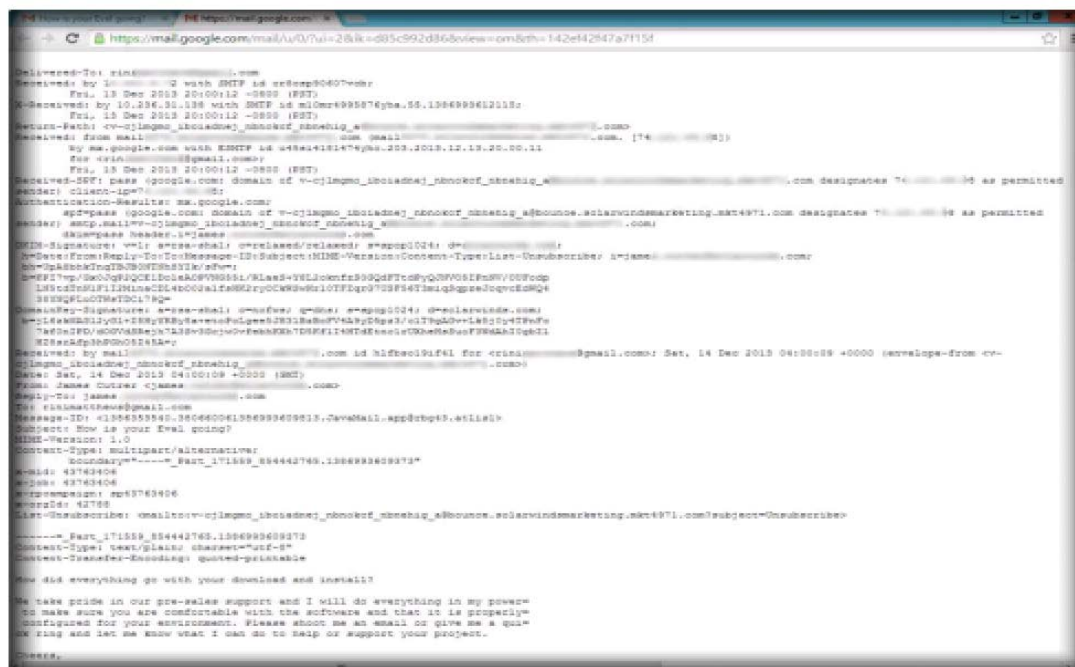


FIGURE 6.6: header appearing tab in browser

15. Copy the entire text and paste it in the **Email headers** field, and click **Trace**.

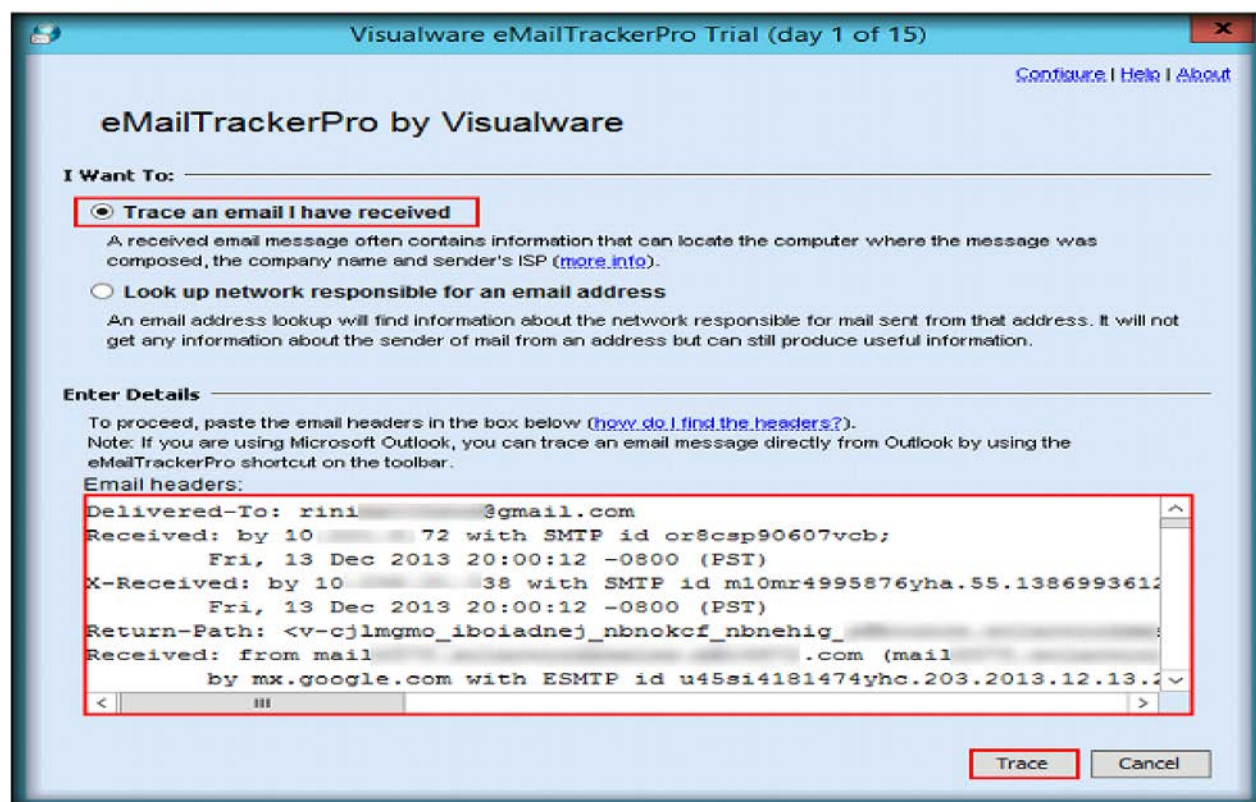


FIGURE 6.7: Email headers and Tracing emails

16. The **My Trace Reports** window opens.
17. The email location is traced in a GUI world map. The location and IP addresses may vary. You can also view the summary by selecting **Email Summary** on the right side of the window.
18. The **Table** section right below the Map shows the entire hop in the route, with the **IP** and suspected locations for each hop.

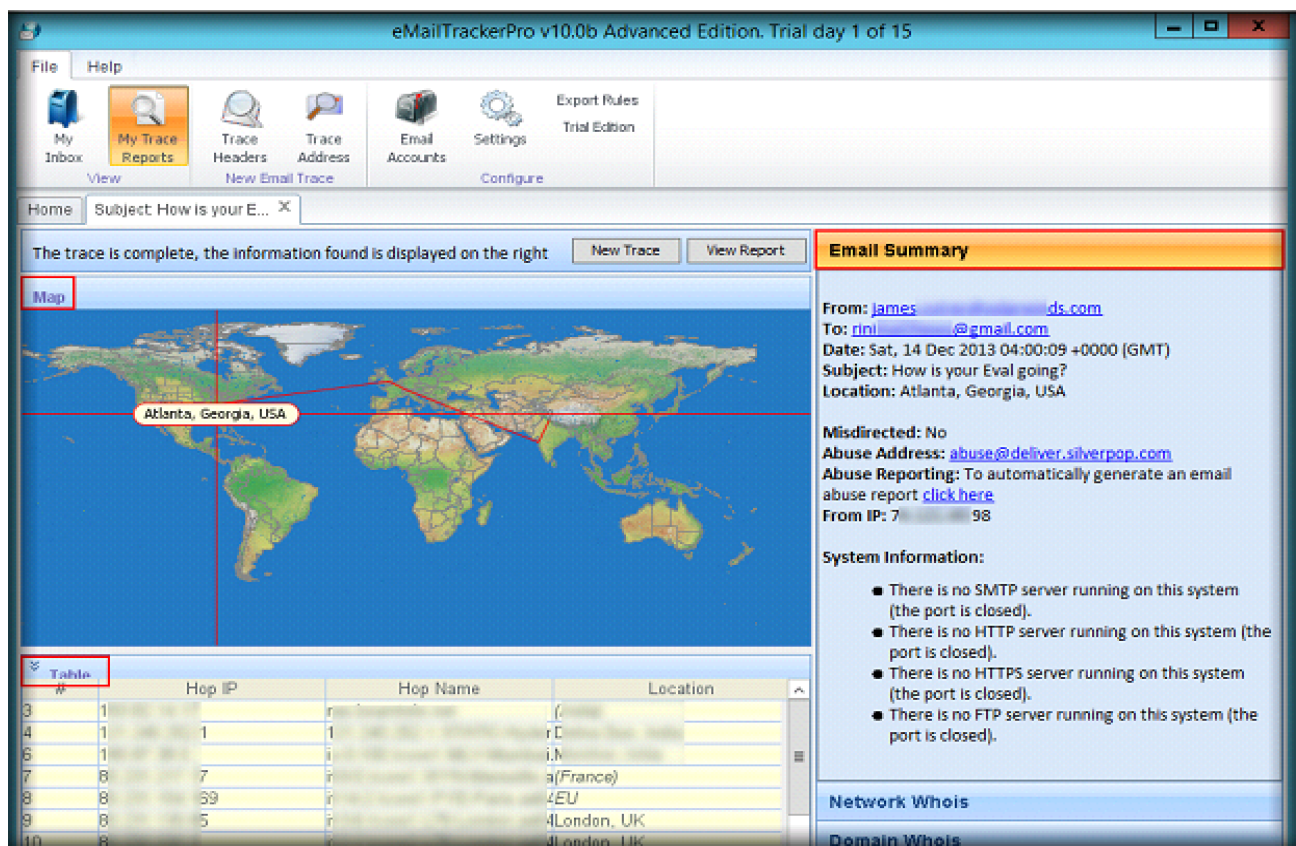


FIGURE 6.8: eMailTrackerPro – Email Trace Report

19. Click **View Report** to view the complete trace report.

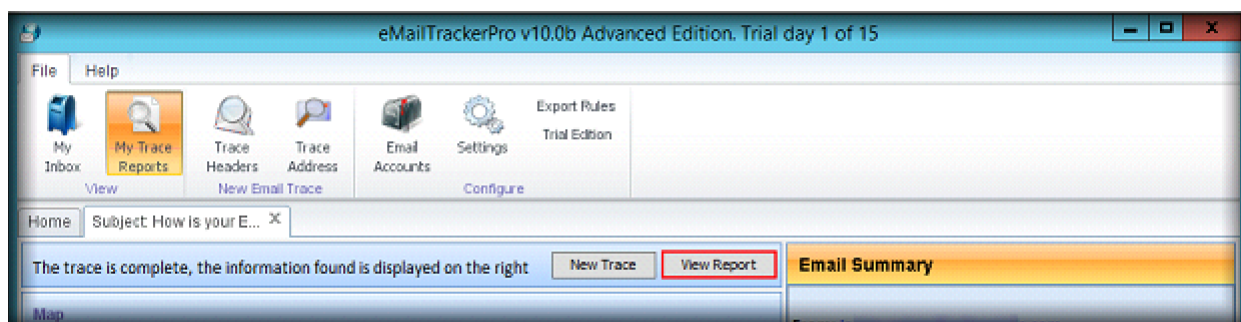


FIGURE 6.9: The eMailTrackerPro - My Trace Reports tab

20. The complete report appears in the default browser.

21. Expand each section to view detailed information.

 **eMailTrackerPro® Report**

[How to Report Email Abuse](#) | [eMailTrackerPro Manual](#) | [FAQ](#) | [Visualware Home](#) | [eMailTrackerPro Website](#) | [Purchase eMailTrackerPro](#)

Identification Report for 'How is your Eval going?'

You are on day 1 of your 15-day trial period. The trial period allows you to try eMailTrackerPro without any obligation. To use eMailTrackerPro after the trial period, you will need to [purchase a product license](#) from the Visualware website or authorized reseller.

Computer 78.128.138.18 has been found. It is almost certainly located in **Atlanta, Georgia, USA** as it has an exact match in the eMailTrackerPro database.

Network Contact Information: The following details refer to the network that the system is on.

 SI Systems Inc.

 abuse@dc.com

 +1-678-500

 200 Galleria Pkwy Ste 750 Atlanta GA 30339 US

Domain Contact Information: The following details refer to a name registered for this address.

 dns admin

 dns.com

 +1-678-26

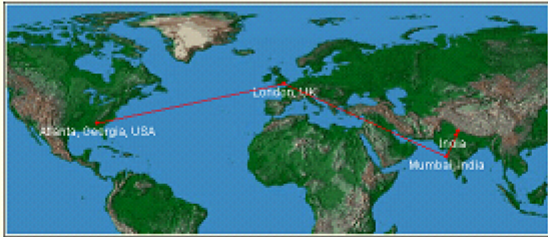
 +1-678-01

☐ [Click here to hide the in-depth information on this email](#) *(more info)*

- The closest tracable IP for this mail was taken from the mail server that the sender first communicated with. The actual sender IP was not added by that server. The closest tracable IP to the sender was - 78.128.138.18
- The sender of this email appeared to have the address james.cutrer@solarwinds.com. This information is easily faked so should not be treated as conclusive.

☐ [Click here to hide the route map](#) *(more info)*

The following map shows the route between you and the entity to which you traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.



☐ [Click here to show information on each hop along the route](#) *(more info)*

☐ [Click here to show further owner details](#) *(more info)*

eMailTrackerPro 10.0a Copyright © Visualware, Inc. 2012

FIGURE 6.10: eMailTrackerPro – detailed information Report

Lab Analysis

Document all the live emails discovered during the lab with all additional information.

Dr Carlene Campbell

Page 10 of 18

Task 2: Scanning Networks - Anonymous Browsing using CyberGhost

Scanning a network refers to a set of procedures for identifying hosts, ports, and services running in a network.

CyberGhost allows you to surf anonymously and access blocked or censored content.

Lab Scenario

As an expert hacker or penetration tester, you should have sound knowledge of different techniques used for anonymous browsing. In this lab, you will learn another way to maintain your Internet anonymity.

Lab Objectives

This lab will help you understand how to use CyberGhost for anonymous browsing.

Pre- Activity exercise

To carry out the lab, you need:

1. Install Windows 7 or Windows 10 in Virtual Box which is on the shared drive as instructed by your tutor.
2. The CyberGhost, located is also on the Shared OneDrive, https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EuNt8HZyAe9MspBMimLvuj4BkzMzBjMCvr1RHRS55ETdTw?e=Xkoeik
3. You can also download the latest version of CyberGhost from this link from https://www.cyberghostvpn.com/en_US/download/windows
4. The latest cyberghost may be a trial version and in some instance may have a name change.
5. Note the screenshot in this lab might differ slightly.
6. Administrative privileges required.

Overview of Email Tracing/Tracking

CyberGhost is a fast simple, and efficient way to protect your online privacy, surf anonymously, and access blocked or censored content. It offers top-notch security and anonymity without being complicated to use or slowing down your Internet connection.

- Whether or not the recipient visited any links sent in the email
- PDFs and other types of attachments
- If messages were set to expire after a specified time.

Activity:

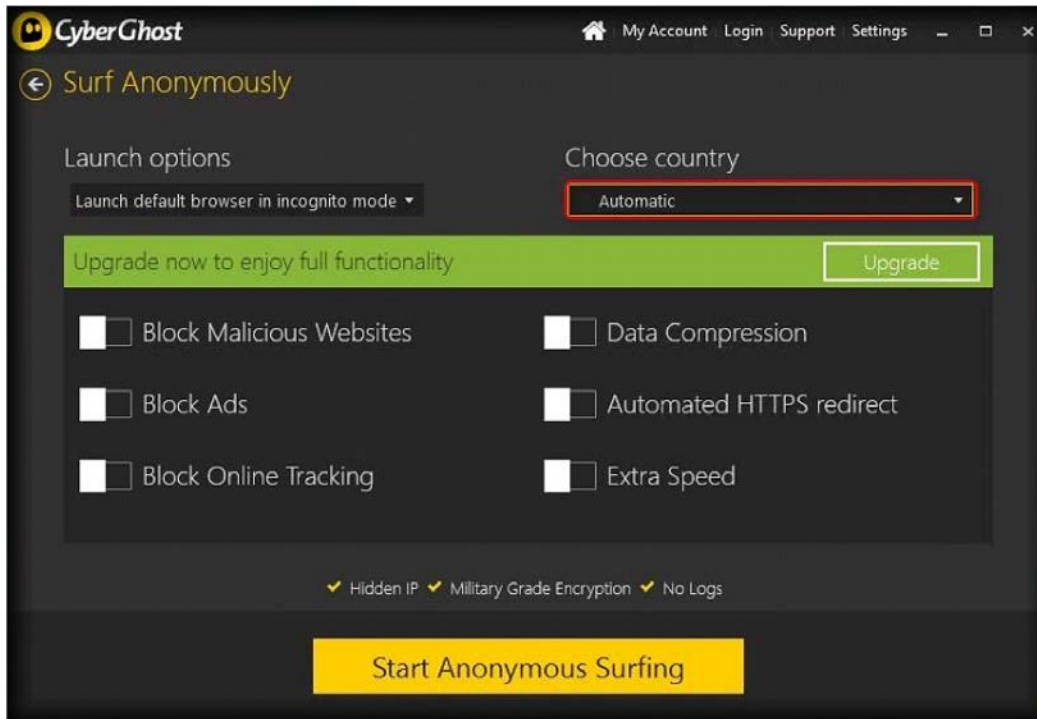
1. Logon to the virtual machine
2. Navigate to the shared OneDrive folder https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uowtsd_ac_uk/EuNt8HZyAe9MspBMimLvvj4BkzMzBjMCvr1RHRS55ETdTw?e=Xkoeik for CyberGhost and double click CG_5.0.13.17.exe
3. If the **Open File – Security Policy** pop-up appears, click Run, then Follow the installation steps to install it on the host machine.
4. Once the installation is complete, the CyberGhost GUI displays the real location of your server, along with its IP address.

Note: An upgrade now Windows opens with the GUI. Close this window. The Real location traced by CyberGhost may differ in you're the lab environment.

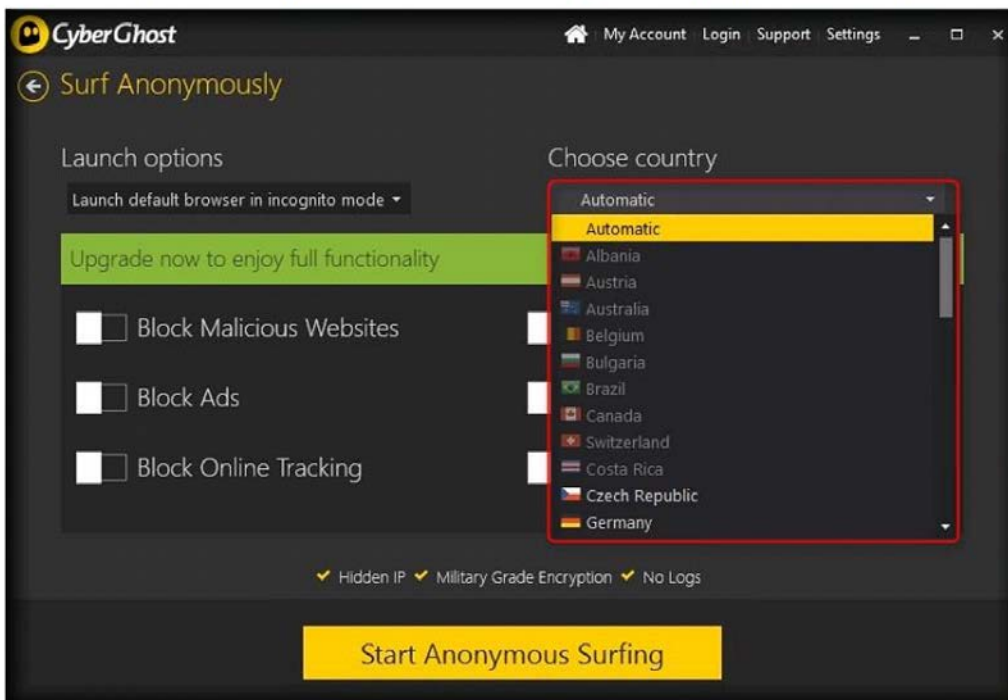
5. Now, click **Surf Anonymously** button in the CyberGhost application window.



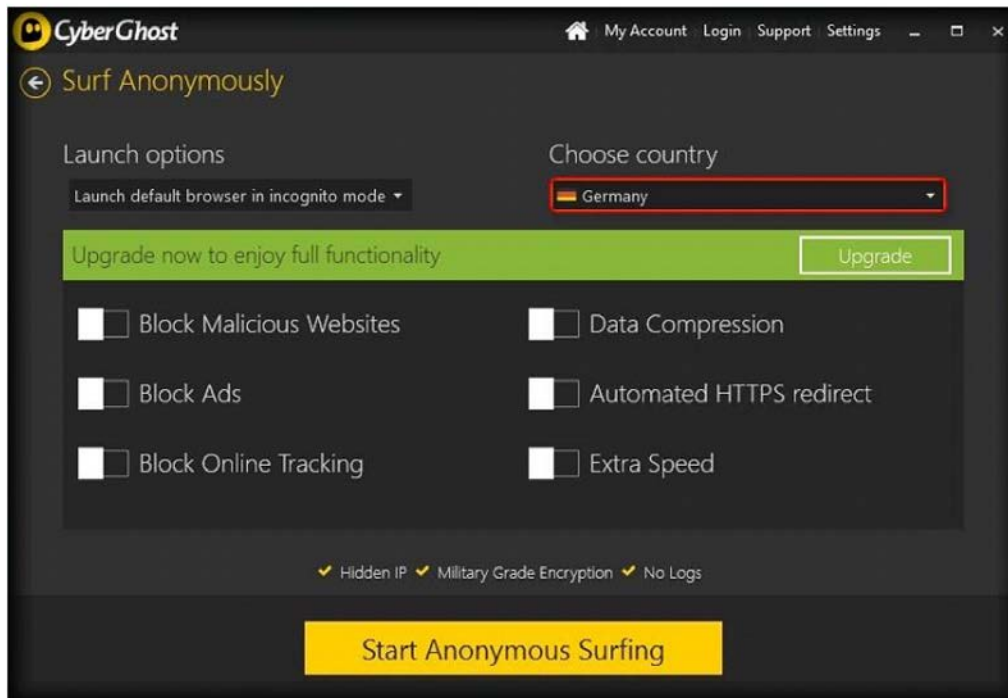
6. Surf Anonymously section appears displaying **Automatic** in the **Choose country** list by default.



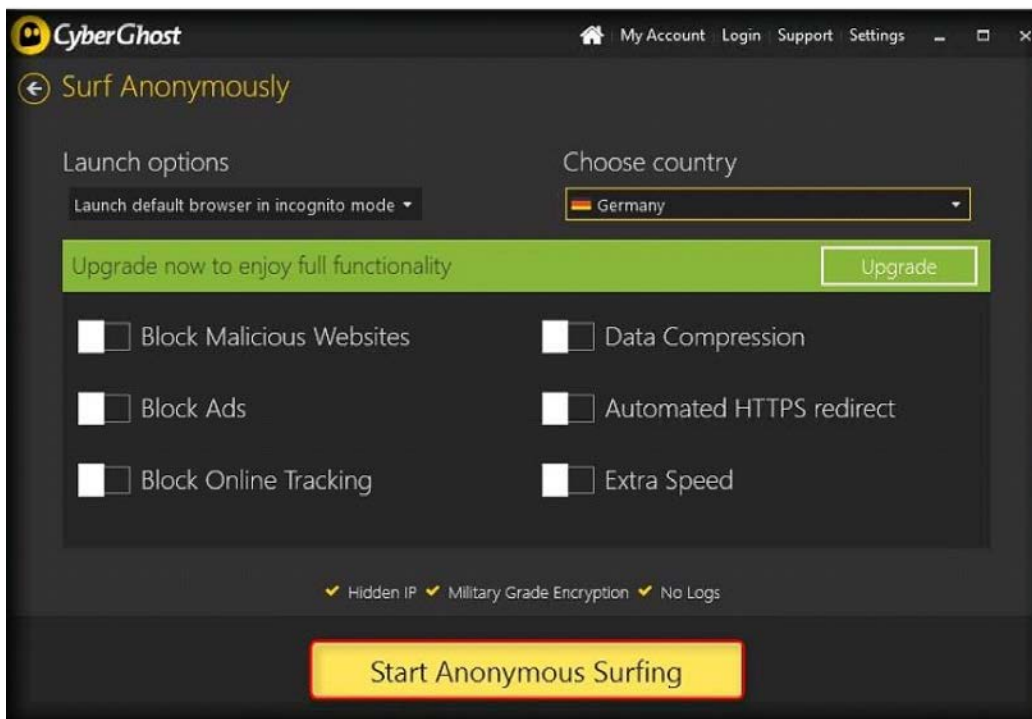
7. Select a country from the list. In this lab, **Germany** has been selected.



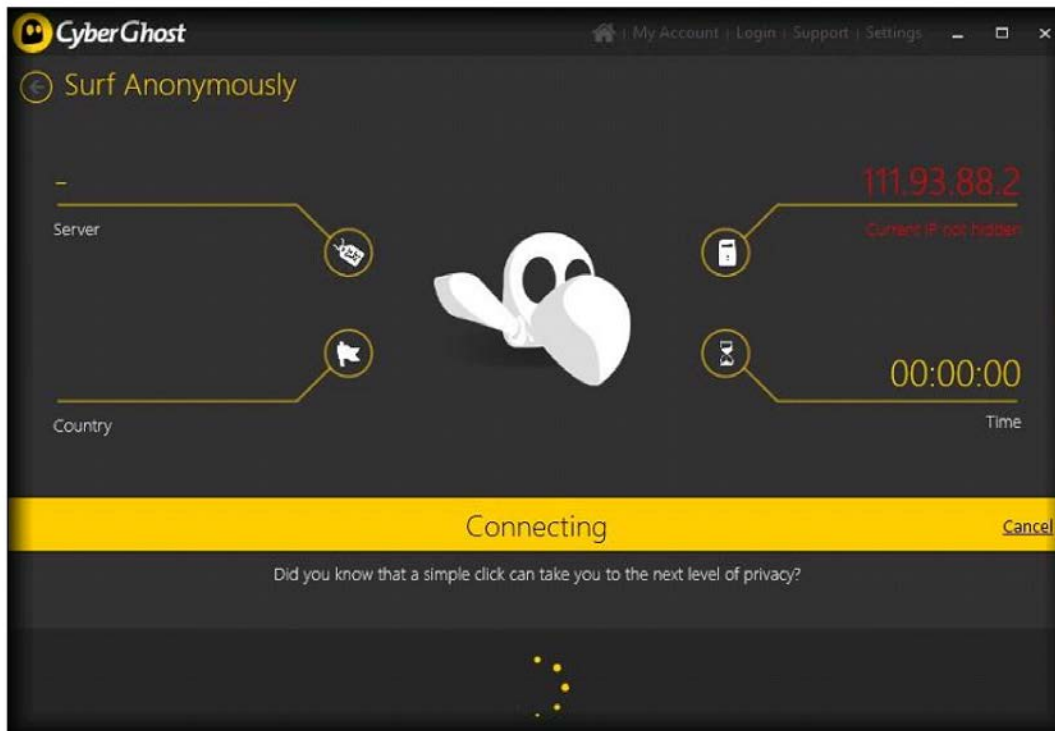
8. The **Choose country** changes to **Germany**, as shown in the following screenshot:



9. Click the **Start Anonymous Surfing** button to initiate **CyberGhost**.

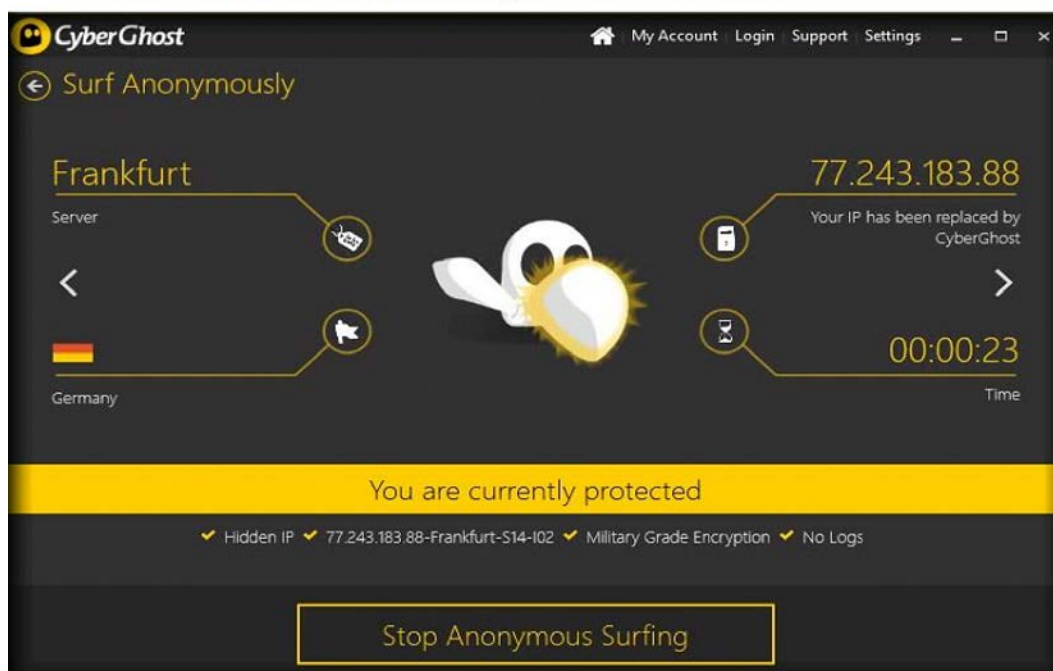


10. **CyberGhost** attempts to establish a connection to the proxy server located in **Germany**, as shown in the following screenshot:



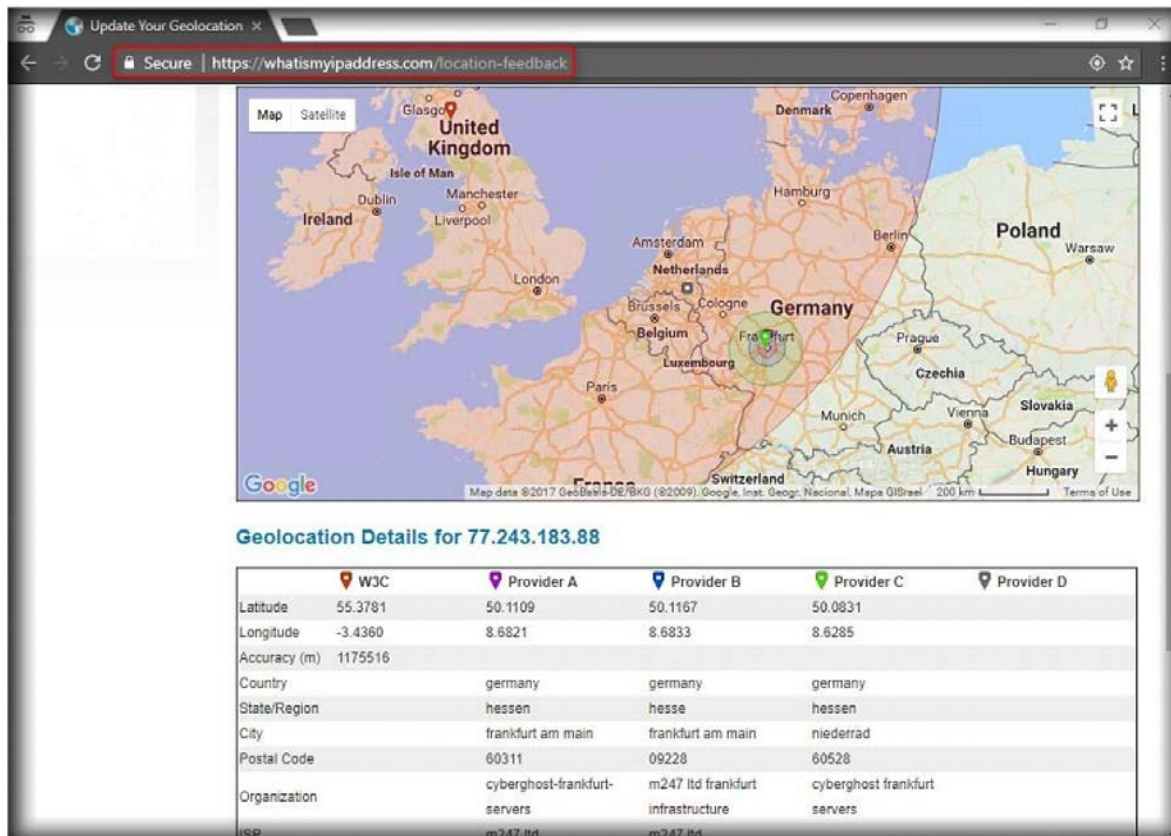
11. On successfully establishing a connection, the simulated location changes to Germany, and the IP address changes to that of the server in Frankfurt, as shown in the following screenshot:

Note: The server may differ in your lab environment.



12. Launch the **Mozilla Firefox** web browser, type the URL **<http://whatismyipaddress.com/location-feedback>** in the address bar, and press **Enter**.

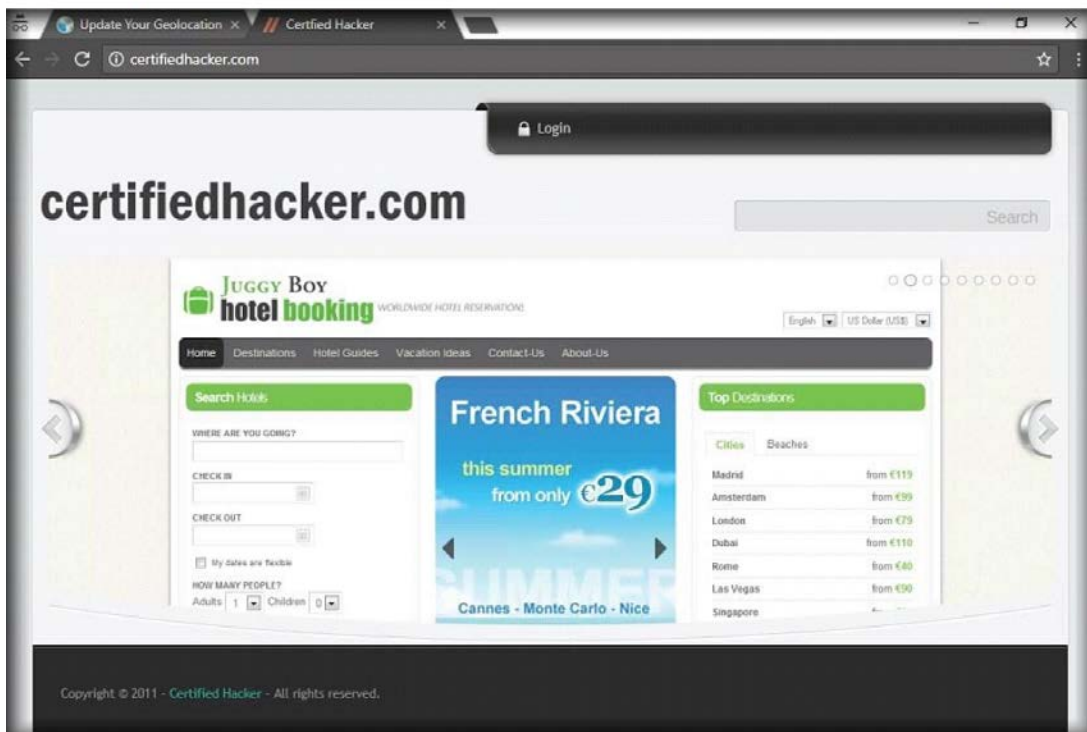
13. Scroll down to the **Geographical Details** section. Observe that the server IP address and location has changed to **77.243.183.88** and **Germany**:



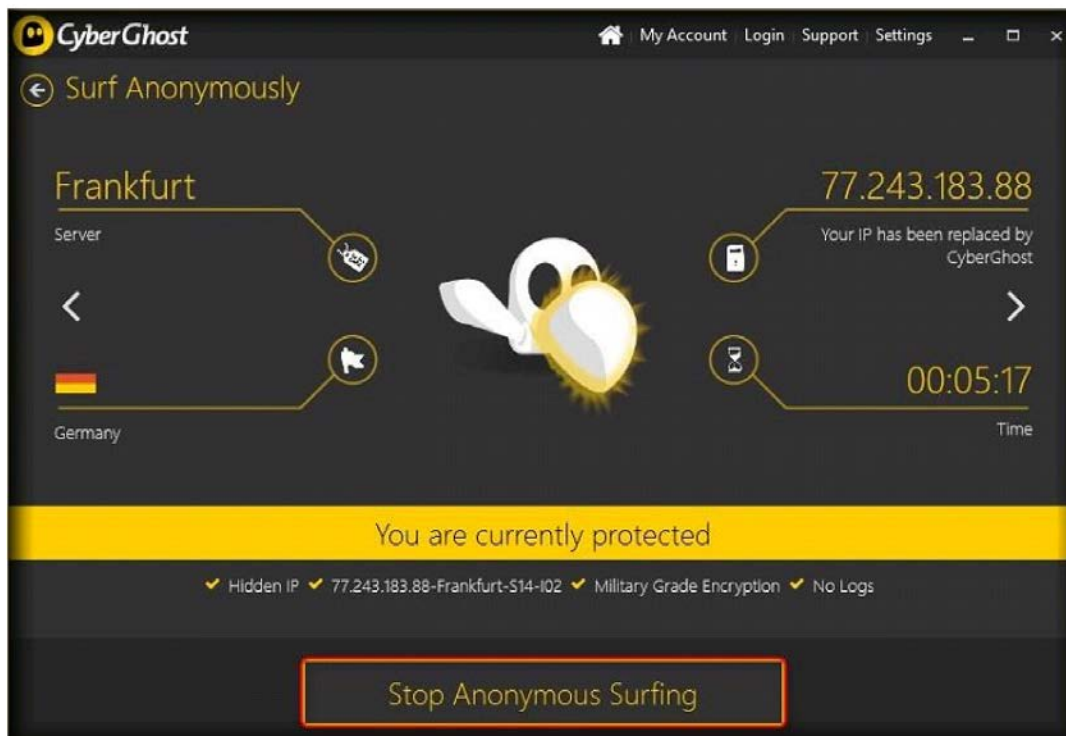
Geolocation Details for 77.243.183.88

	W3C	Provider A	Provider B	Provider C	Provider D
Latitude	55.3781	50.1109	50.1167	50.0831	
Longitude	-3.4360	8.6821	8.6833	8.6285	
Accuracy (m)	1175516				
Country		germany	germany	germany	
State/Region		hessen	hesse	hessen	
City		frankfurt am main	frankfurt am main	niederrad	
Postal Code		60311	09228	60528	
Organization		cyberghost-frankfurt-servers	m247 ltd frankfurt infrastructure	cyberghost frankfurt servers	
ISP		m247 ltd	m247 ltd		

14. Open a new tab in a **web browser**, and surf anonymously using this proxy.



15. Once you are done browsing, click the **Stop Anonymous Surfing** button again to disconnect the proxy. **CyberGhost** now displays your real location, as shown in the following screenshot:



Lab Analysis

Document all the IP address of live (SSL) proxy servers and the connectivity you discovered during this lab.