Practice Labs - Ethical Hacker v10

Sniffing

Introduction

MAC Address
MAC Address Changer
SMAC
Wireshark
PromqryUI
Cain and Abel
Sniff-O-Matic
Ethical Hacking

Welcome to the **Sniffing** Practice Lab. In this module, you will be provided with the instructions and devices needed to develop your hands-on skills.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Sniffing Techniques and Analysis
- Exercise 2 - Sniffing Prevention Techniques

After completing this lab, you will be able to:

- Use MAC Address Changer: Change MAC Address
- Use SMAC 2.0
- Install Wireshark
- Use Wireshark
- Use Sniff-O-Matic
- Use XArp Utility

Exam Objectives

The following exam objectives are covered in this lab:

- **3.2** Information Security Attack Detection
- **3.3** Information Security Attack Prevention

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **1 hour** to complete this lab.

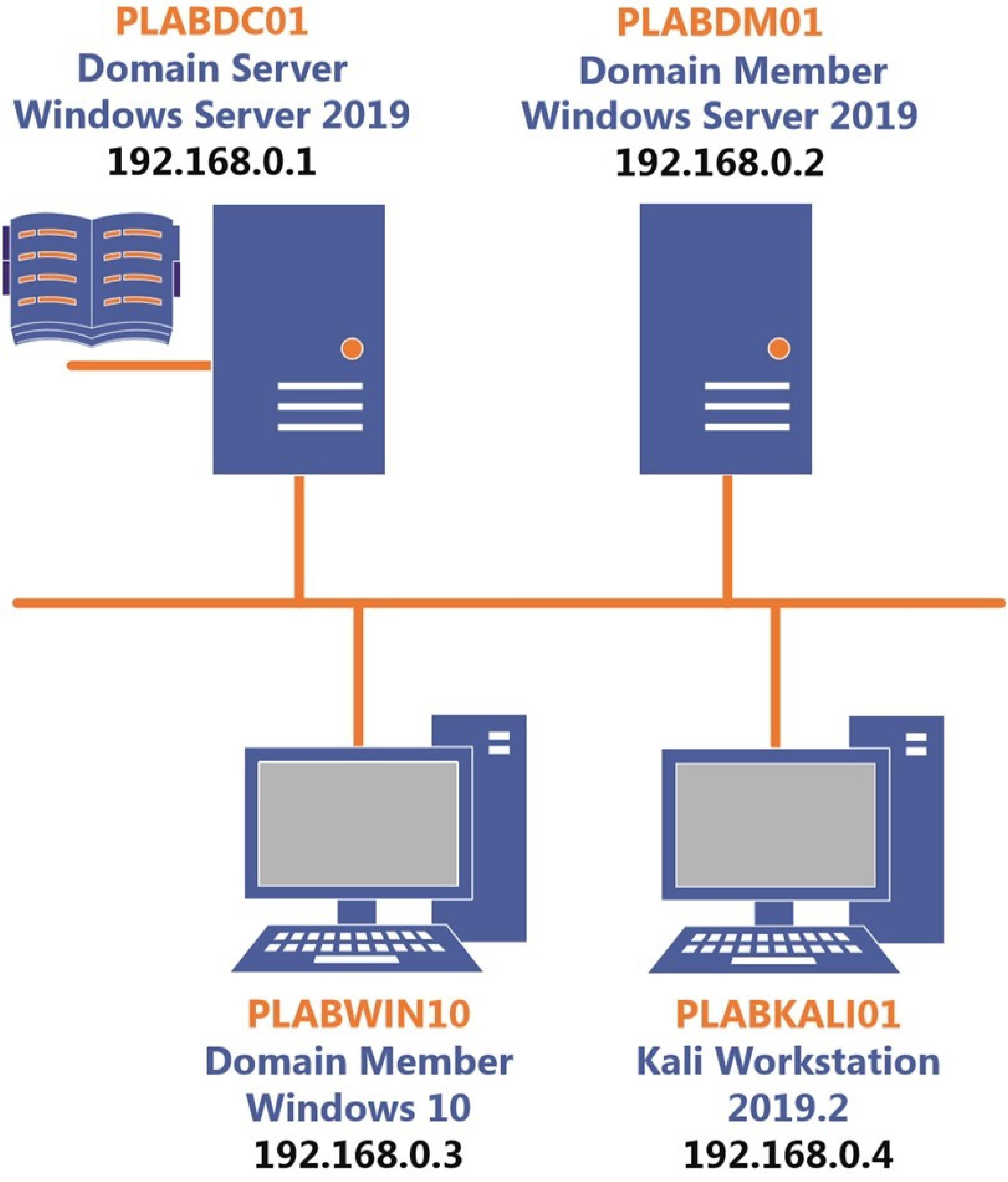
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

During your session, you will have access to the following lab configuration.



Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Member)
- **PLABWIN10 -** (Windows 10 - Workstation)
- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)

Click **Next** to proceed to the first exercise.

Exercise 1 - Sniffing Techniques and Analysis

Sniffing refers to the process in which data packets traveling over a network are captured, and a network adapter that is configured to promiscuous mode can capture packets in transit. Sniffed packets can then be reviewed using a tool, such as Wireshark.

In this exercise, you will learn to perform various types of sniffing.

Learning Outcomes

After completing this exercise, you will be able to:

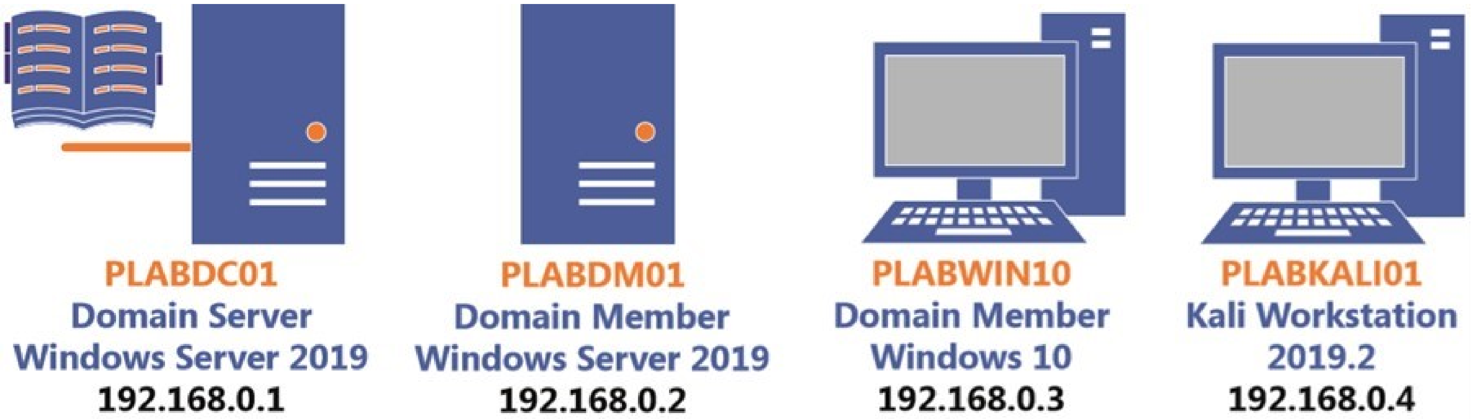
- Use MAC Address Changer: Change MAC Address
- Use SMAC 2.0
- Install Wireshark
- Use Wireshark
- Use Sniff-O-Matic

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABDM01 -** (Windows Server 2019 - Domain Member)
- **PLABWIN10 -** (Windows 10 - Workstation)

- **PLABKALI01 -** (Kali 2019.2 - Linux Kali Workstation)



Task 1 - Use MAC Address Changer: Change MAC Address

Using **Change MAC Address**, you can change the **MAC** address of your system. You can also configure it to use the **MAC** address of random **Network Interface Card** (**NIC**) manufacturers.

In this task, you will learn to use **Change MAC Address**. To do this, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10.**

In the **Type here to search** text box, type the following:

```
Internet Explorer
```

From the search results, select **Internet Explorer**.

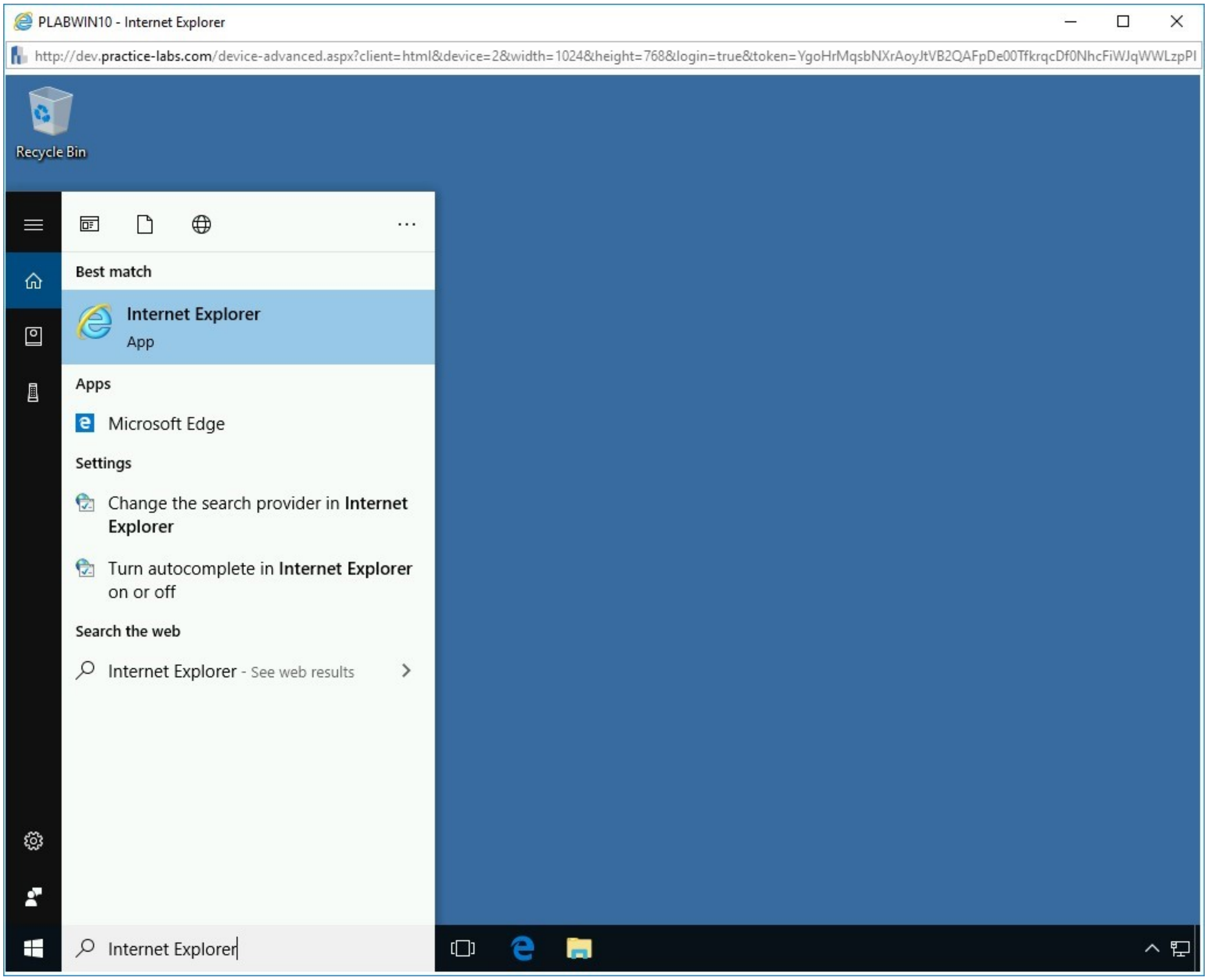
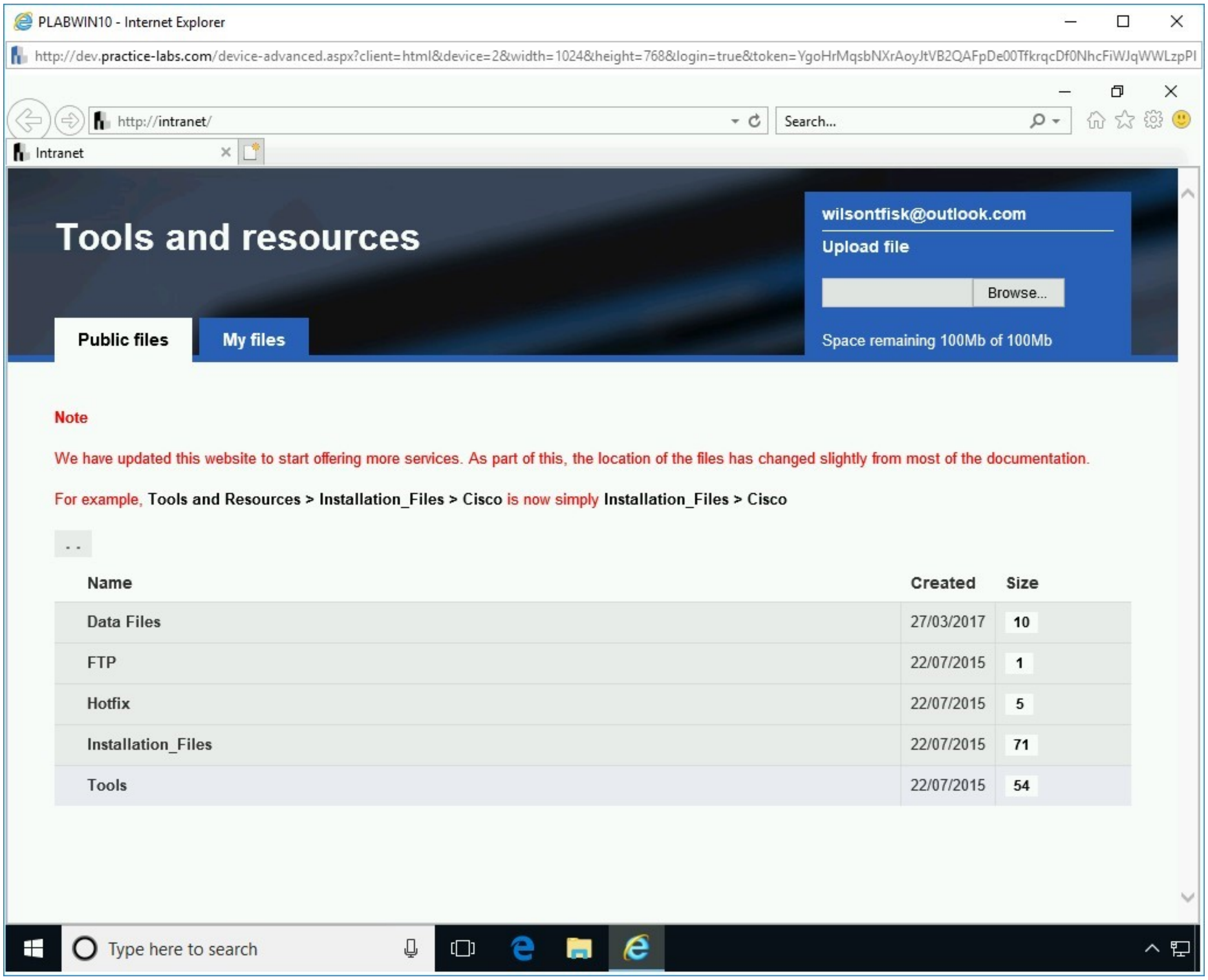

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Recycle Bin
Best match
Internet Explorer
App
Apps
Microsoft Edge
Settings
Change the search provider in Internet Explorer
Turn autocomplete in Internet Explorer on or off
Search the web
Internet Explorer - See web results
Internet Explorer

Figure 1.1 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 2

Internet Explorer opens the **Tools and resources** Webpage.

Click **Tools**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, Tools and Resources > Installation_Files > Cisco is now simply Installation_Files > Cisco

. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	71
Tools	22/07/2015	54

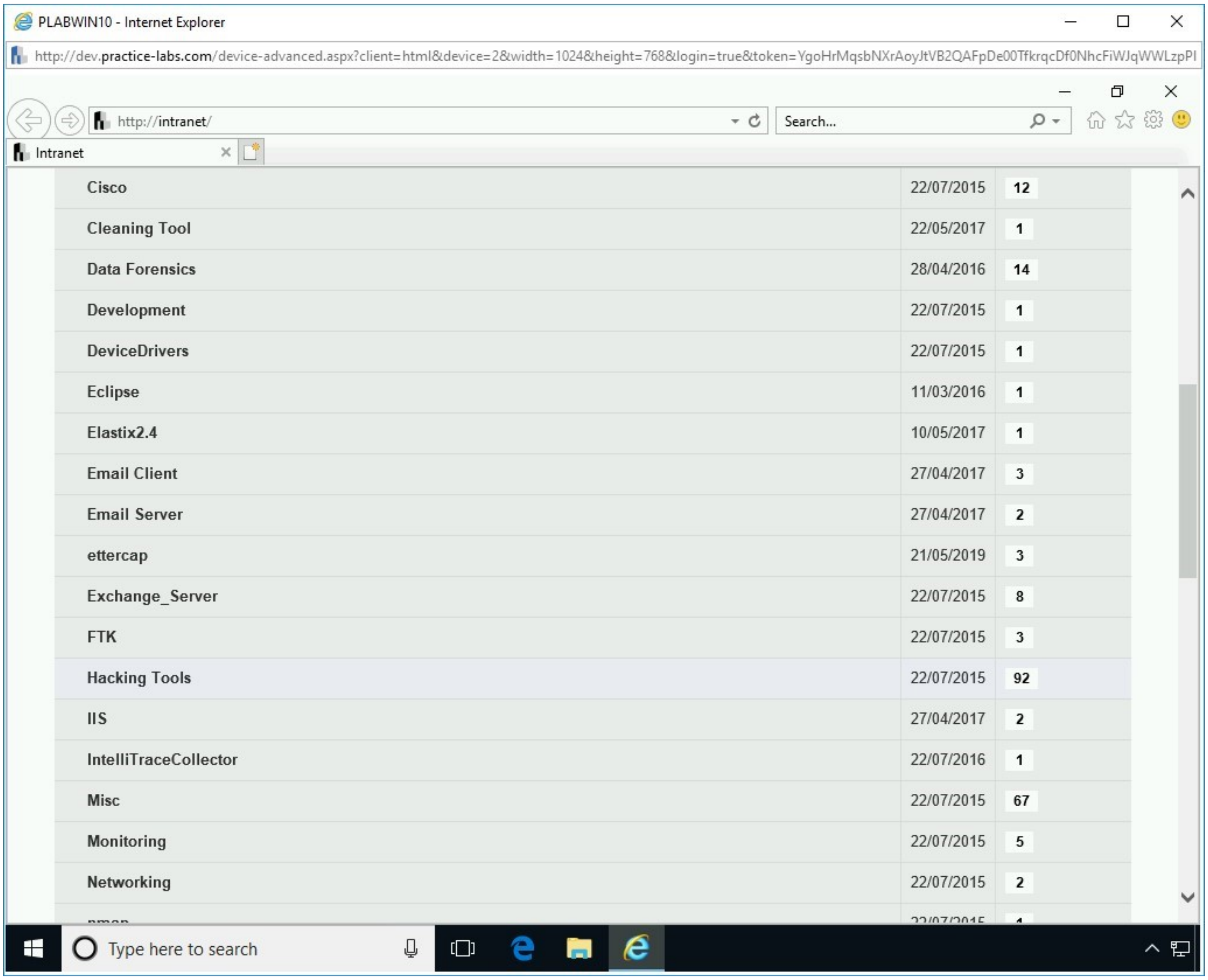
Figure 1.2 Screenshot of PLABWIN10: Internet Explorer Intranet page is displayed. Clicking the Tools option on the Tools and resources page.

Step 3

You will be directed to **[..] > Tools**.

Scroll down a bit and locate **Hacking Tools**.

Click **Hacking Tools**.

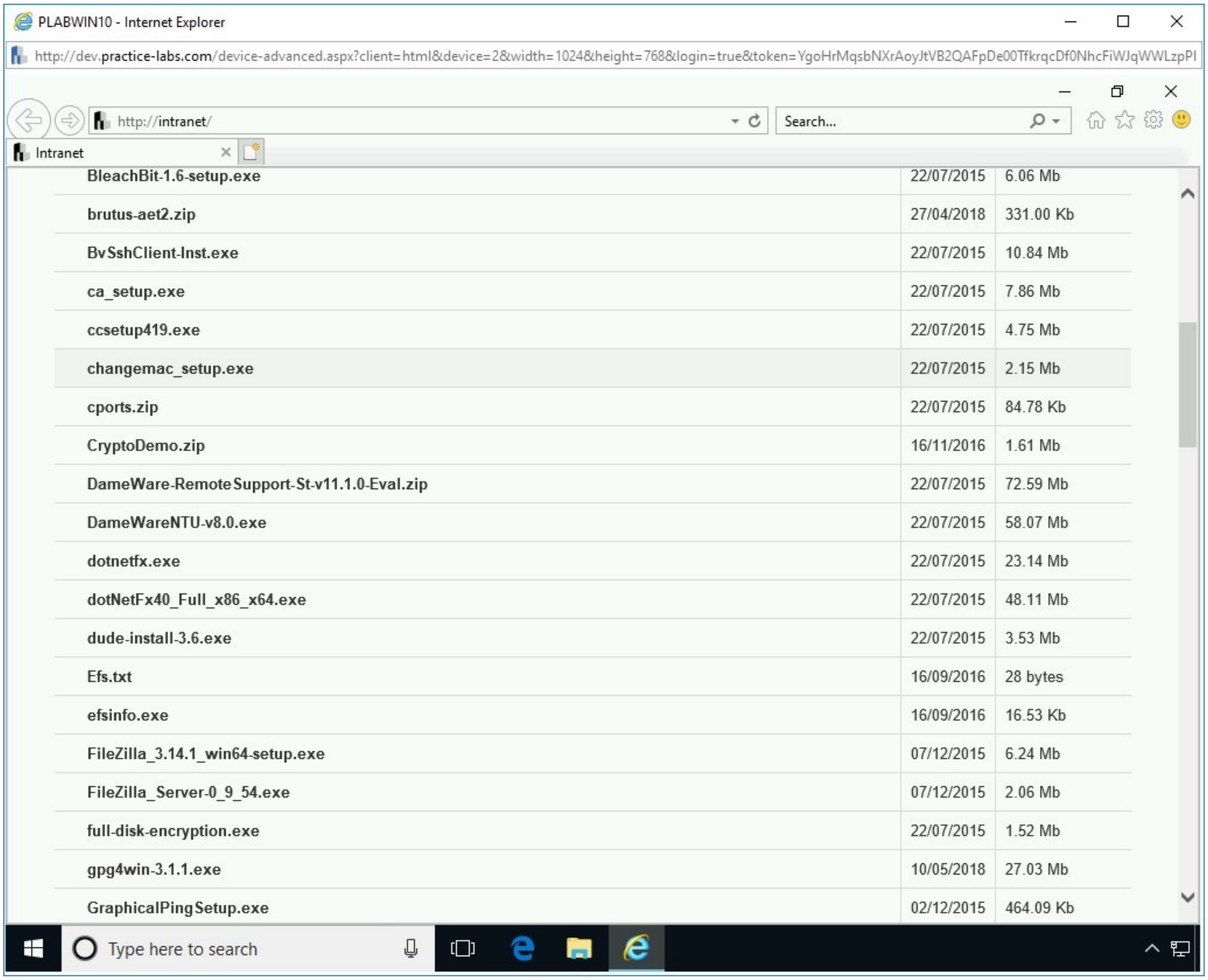

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
Type here to search

Cisco	22/07/2015	12
Cleaning Tool	22/05/2017	1
Data Forensics	28/04/2016	14
Development	22/07/2015	1
DeviceDrivers	22/07/2015	1
Eclipse	11/03/2016	1
Elastix2.4	10/05/2017	1
Email Client	27/04/2017	3
Email Server	27/04/2017	2
ettercap	21/05/2019	3
Exchange_Server	22/07/2015	8
FTK	22/07/2015	3
Hacking Tools	22/07/2015	92
IIS	27/04/2017	2
IntelliTraceCollector	22/07/2016	1
Misc	22/07/2015	67
Monitoring	22/07/2015	5
Networking	22/07/2015	2
nmap	22/07/2015	1

Figure 1.3 Screenshot of PLABWIN10: Clicking the Hacking Tools option.

Step 4

On the **[..] > Tools > Hacking Tools** page, locate the **changemac_setup.exe** and click on it.

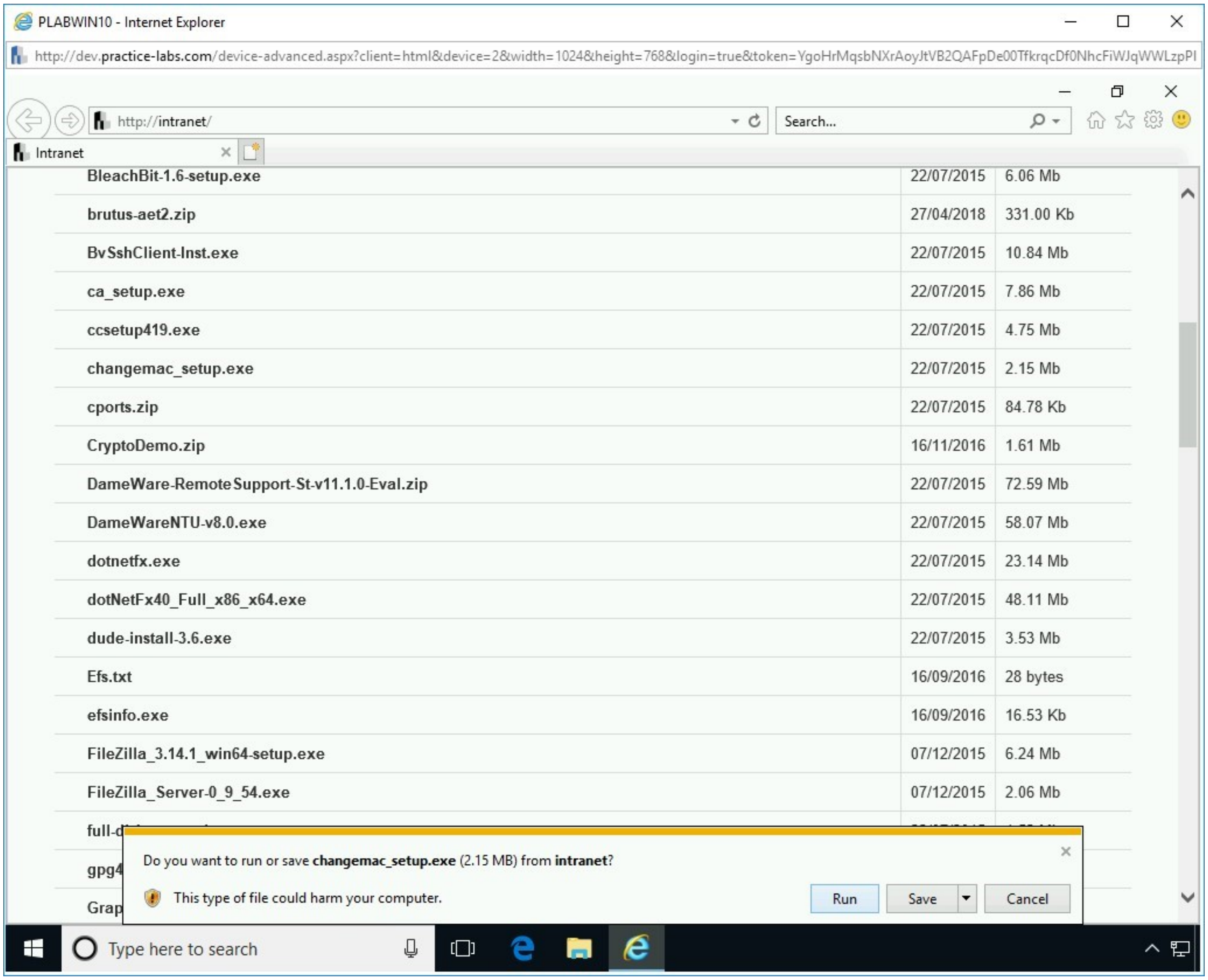

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
Type here to search

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St-v11.1.0-Eval.zip	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Figure 1.4 Screenshot of PLABWIN10: Clicking the changemac_setup.exe file.

Step 5

In the notification bar, click **Run**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Type here to search

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St-v11.1.0-Eval.zip	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-d		
gpg4		
Grap		

Do you want to run or save **changemac_setup.exe** (2.15 MB) from **intranet**?

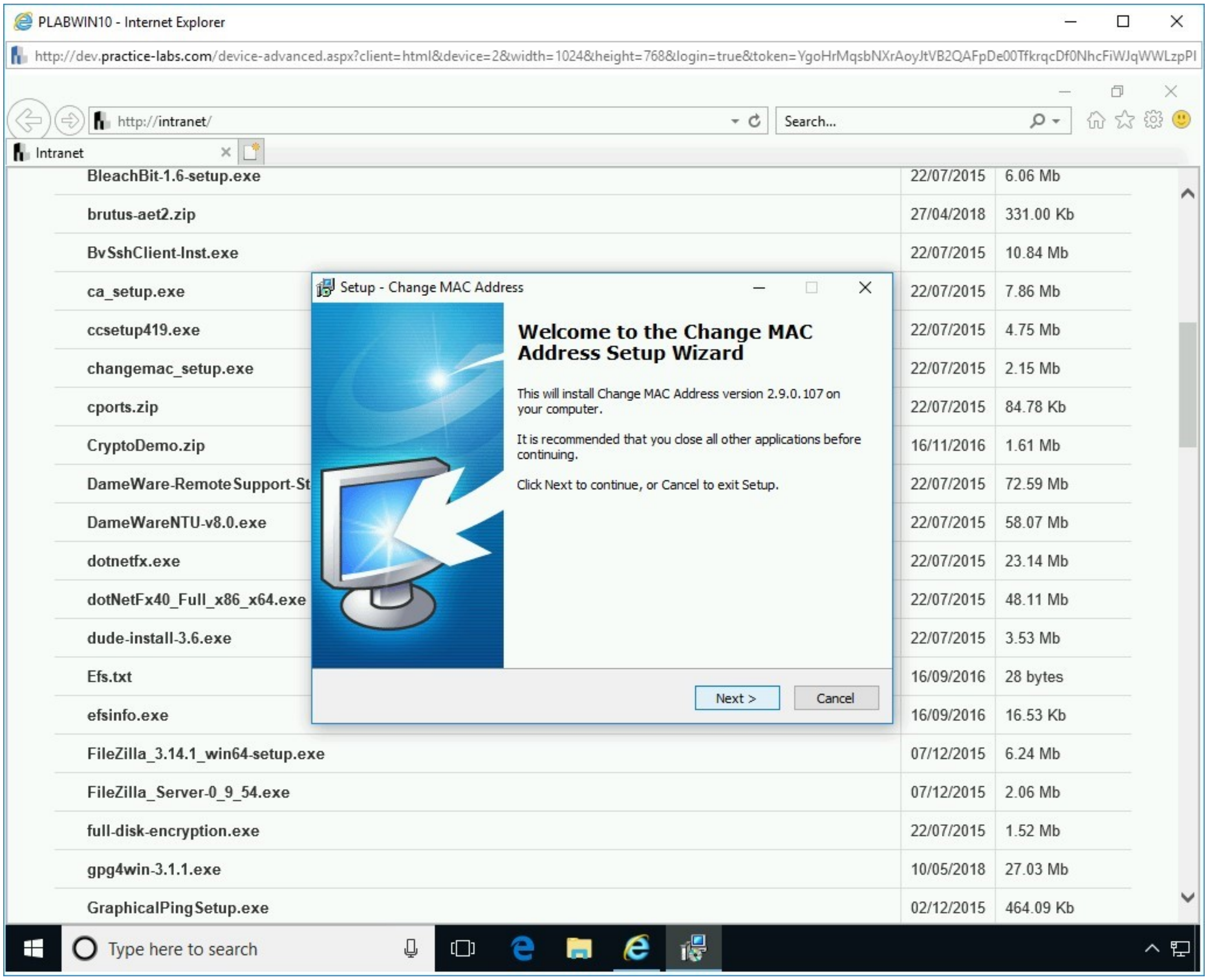
This type of file could harm your computer.

Run | Save | Cancel

Figure 1.5 Screenshot of PLABWIN10: Clicking Run on the notification bar.

Step 6

The **Setup - Change MAC Address** wizard appears. On the **Welcome to the Change MAC Address Setup Wizard** page, click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Next >
Cancel
Type here to search

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Setup - Change MAC Address

Welcome to the Change MAC Address Setup Wizard

This will install Change MAC Address version 2.9.0.107 on your computer.

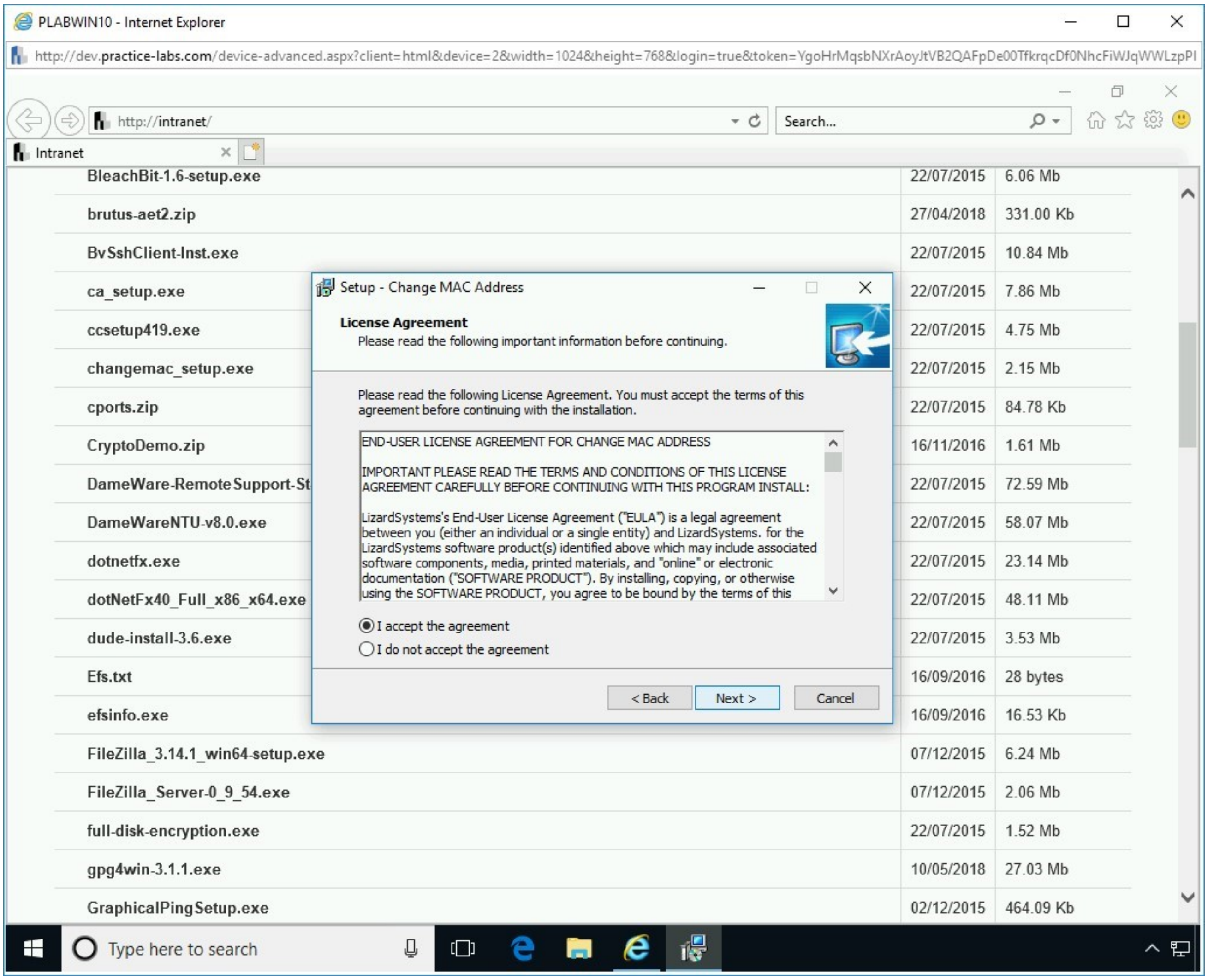
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 1.6 Screenshot of PLABWIN10: Clicking Next on the welcome page of the installation wizard.

Step 7

On the **License Agreement** page, select **I accept the agreement** and click **Next**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

http://intranet/

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Setup - Change MAC Address

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

END-USER LICENSE AGREEMENT FOR CHANGE MAC ADDRESS

IMPORTANT PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE CONTINUING WITH THIS PROGRAM INSTALL:

LizardSystems's End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and LizardSystems. for the LizardSystems software product(s) identified above which may include associated software components, media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this

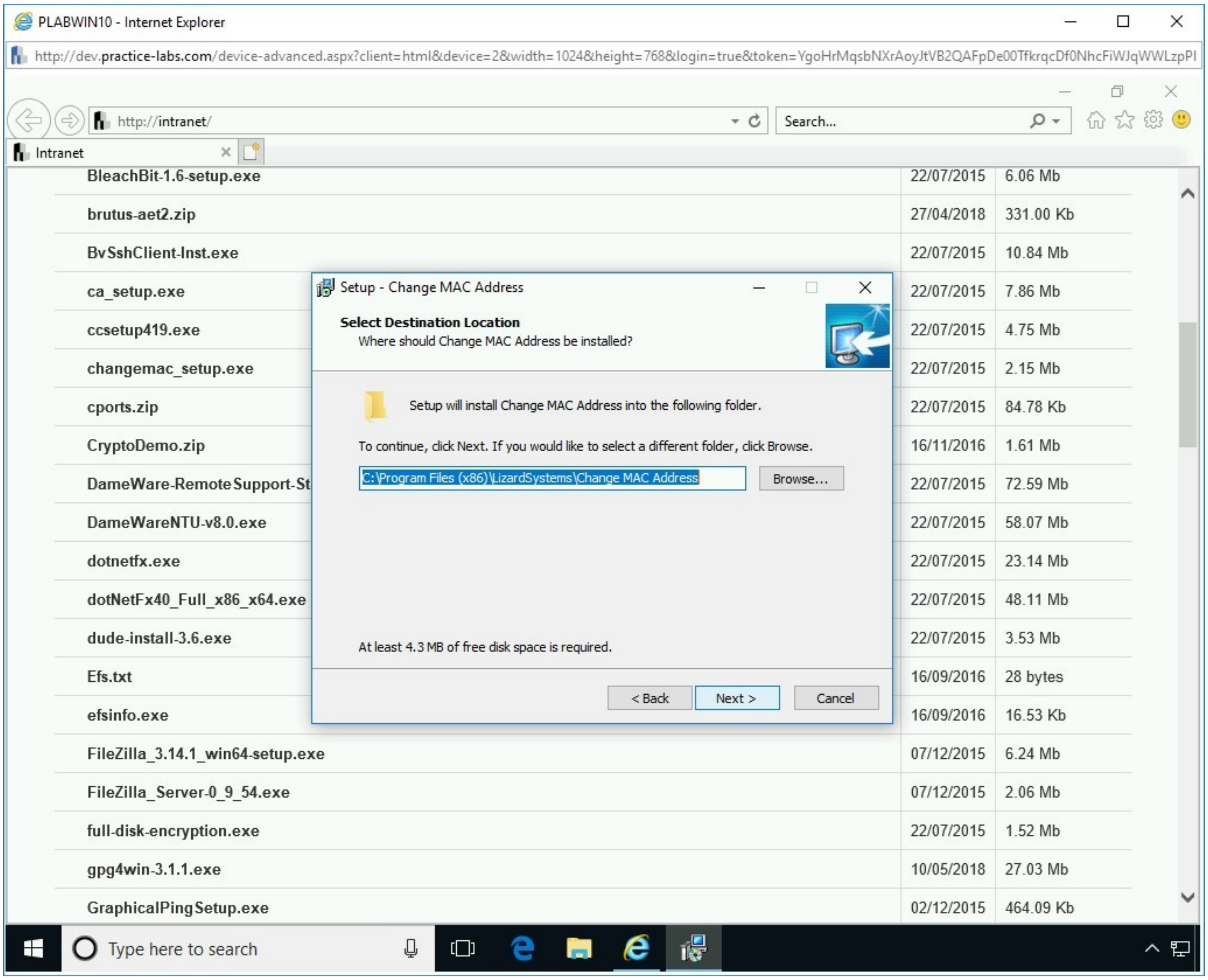
● I accept the agreement

○ I do not accept the agreement

Figure 1.7 Screenshot of PLABWIN10: Selecting I accept the agreement on the license agreement dialog box and clicking Next.

Step 8

On the **Select Destination Location** page, keep the default location and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Browse...
< Back
Next >
Cancel
Type here to search

Setup - Change MAC Address

Select Destination Location

Where should Change MAC Address be installed?

Setup will install Change MAC Address into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\LizardSystems\Change MAC Address

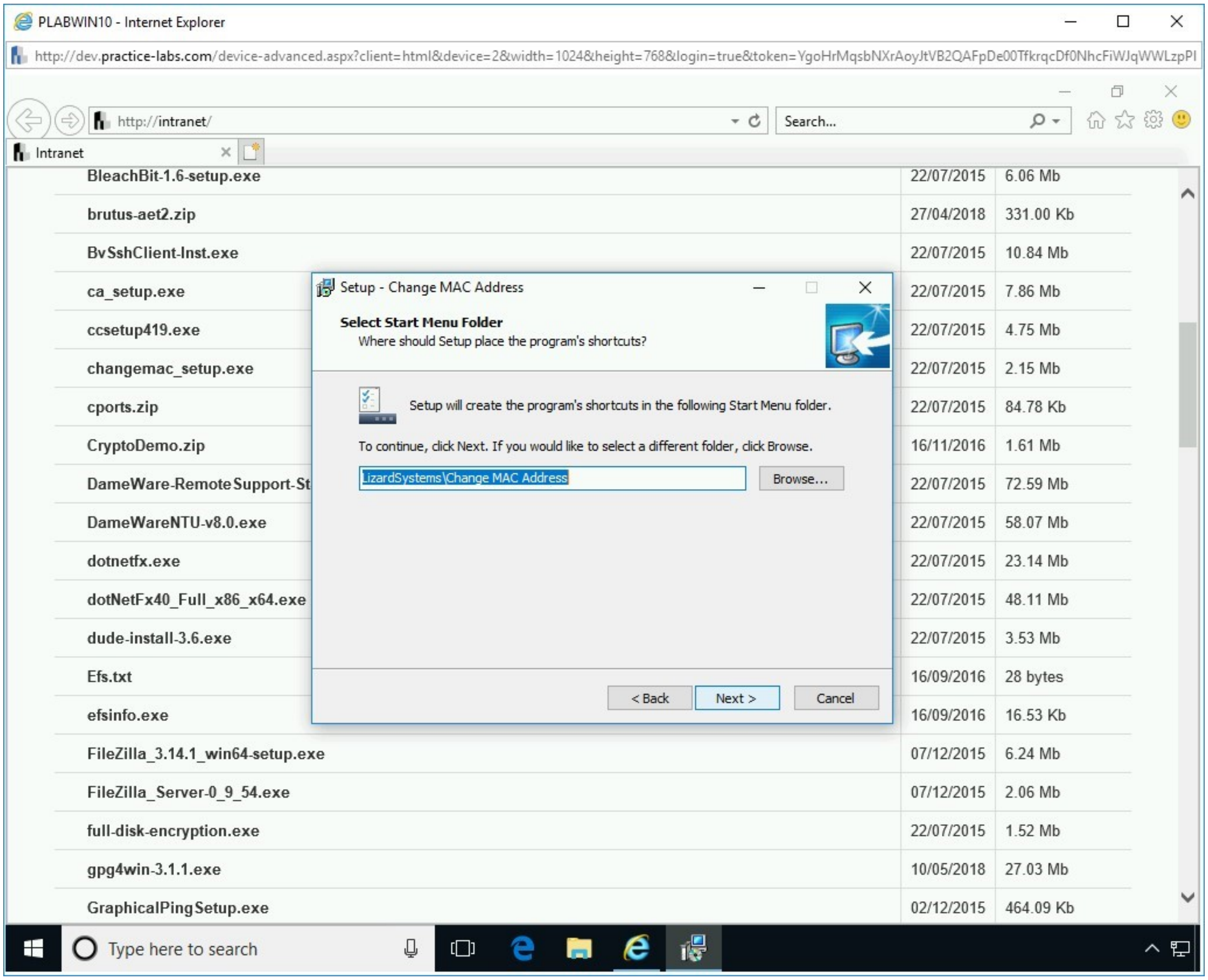
At least 4.3 MB of free disk space is required.

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Figure 1.8 Screenshot of PLABWIN10: Keeping the default installation path and clicking Next on the Select Destination Location page.

Step 9

On the **Select Start Menu Folder** page, keep the default menu name and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
Type here to search

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Setup - Change MAC Address

Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

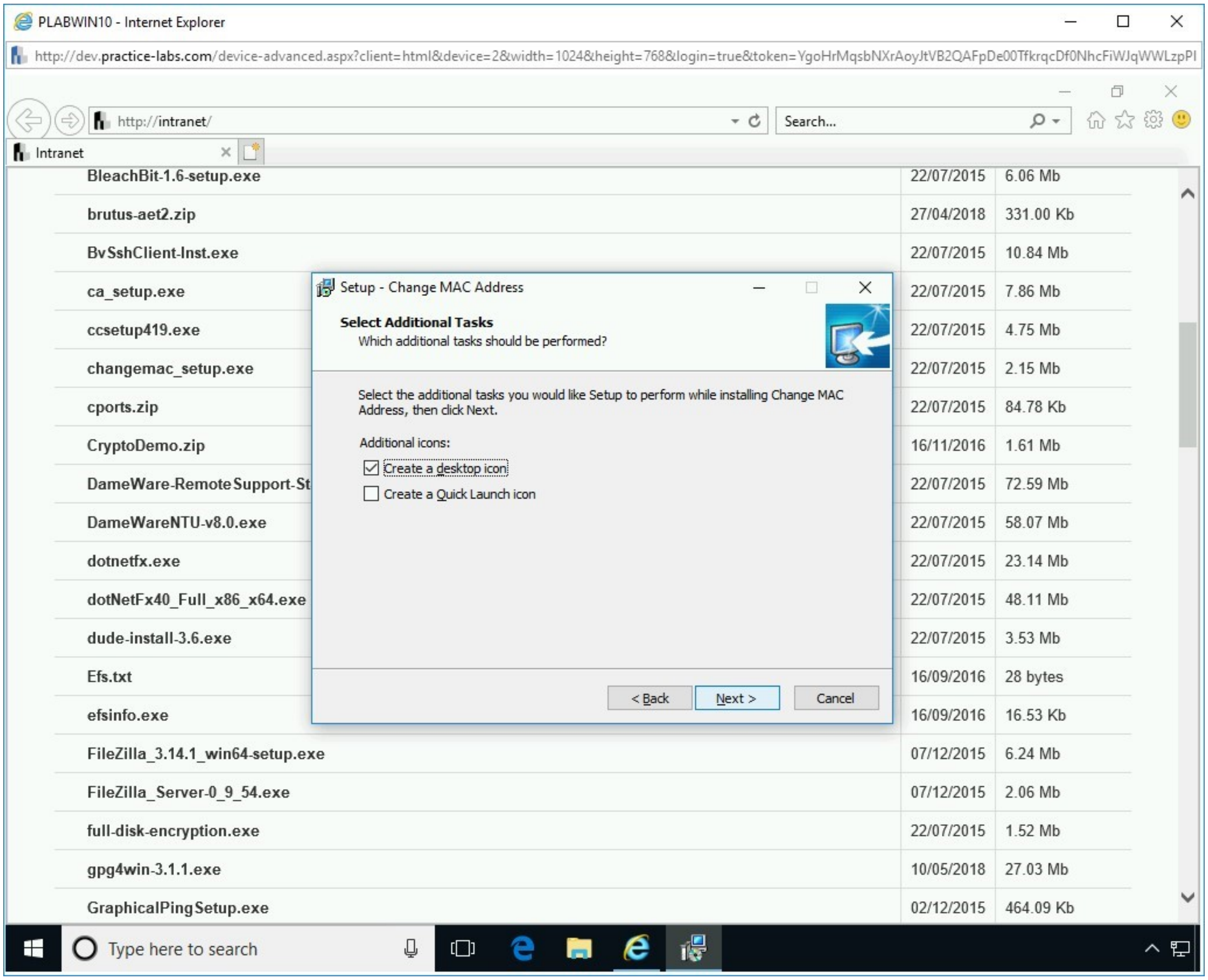
To continue, click Next. If you would like to select a different folder, click Browse.

LizardSystems\Change MAC Address

Figure 1.9 Screenshot of PLABWIN10: Keeping the default menu option name and clicking Next on the Select Start Menu Folder page.

Step 10

On the **Select Additional Tasks** page, keep the default selection and click **Next**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI

http://intranet/

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Setup - Change MAC Address

Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Change MAC Address, then click Next.

Additional icons:

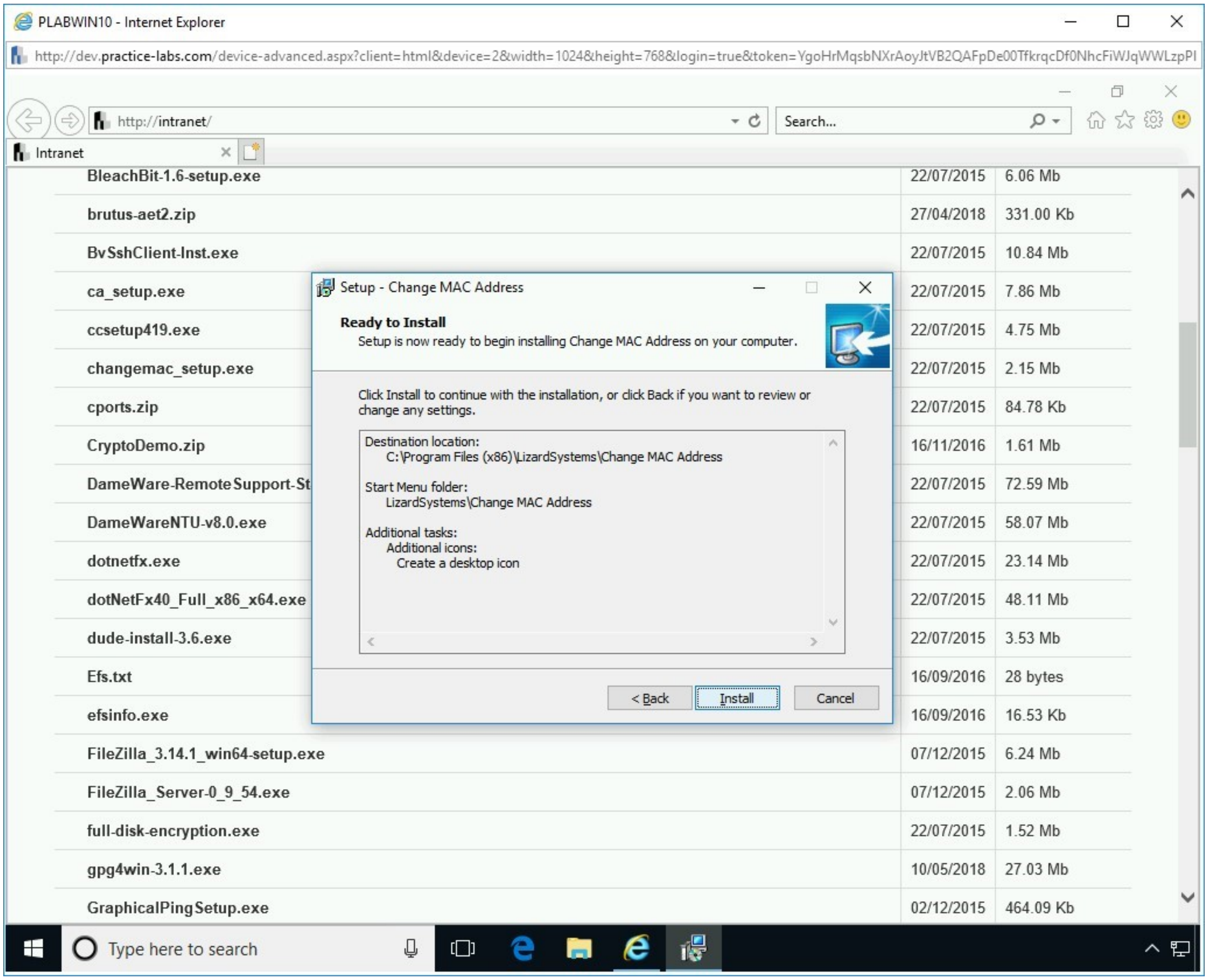
☑ Create a desktop icon

□ Create a Quick Launch icon

Figure 1.10 Screenshot of PLABWIN10: Keeping the default options and clicking Next on the Select Additional Tasks page.

Step 11

On the **Ready to Install** page, review the installation settings, and click **Install**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
Type here to search

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Setup - Change MAC Address

Ready to Install

Setup is now ready to begin installing Change MAC Address on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files (x86)\LizardSystems\Change MAC Address

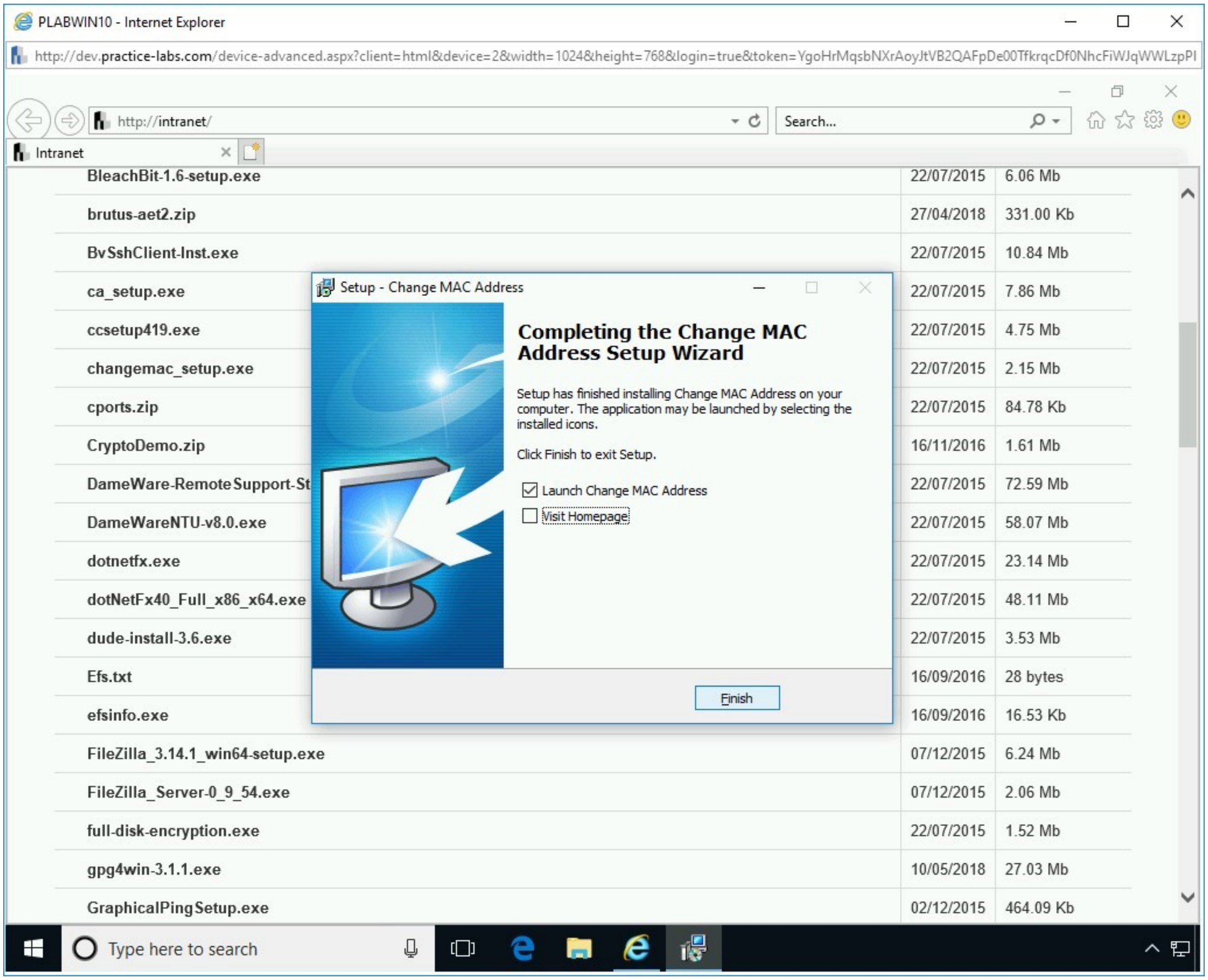
Start Menu folder:
LizardSystems\Change MAC Address

Additional tasks:
Additional icons:
Create a desktop icon

Figure 1.11 Screenshot of PLABWIN10: Clicking Install to start the installation on the Ready to Install page.

Step 12

The installation completes quickly. On the **Completing the Change MAC Address Setup Wizard** page, deselect **Visit Homepage** and click **Finish**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Setup - Change MAC Address
Finish
Type here to search

BleachBit-1.6-setup.exe	22/07/2015	6.06 Mb
brutus-aet2.zip	27/04/2018	331.00 Kb
BvSshClient-Inst.exe	22/07/2015	10.84 Mb
ca_setup.exe	22/07/2015	7.86 Mb
ccsetup419.exe	22/07/2015	4.75 Mb
changemac_setup.exe	22/07/2015	2.15 Mb
cports.zip	22/07/2015	84.78 Kb
CryptoDemo.zip	16/11/2016	1.61 Mb
DameWare-RemoteSupport-St	22/07/2015	72.59 Mb
DameWareNTU-v8.0.exe	22/07/2015	58.07 Mb
dotnetfx.exe	22/07/2015	23.14 Mb
dotNetFx40_Full_x86_x64.exe	22/07/2015	48.11 Mb
dude-install-3.6.exe	22/07/2015	3.53 Mb
Efs.txt	16/09/2016	28 bytes
efsinfo.exe	16/09/2016	16.53 Kb
FileZilla_3.14.1_win64-setup.exe	07/12/2015	6.24 Mb
FileZilla_Server-0_9_54.exe	07/12/2015	2.06 Mb
full-disk-encryption.exe	22/07/2015	1.52 Mb
gpg4win-3.1.1.exe	10/05/2018	27.03 Mb
GraphicalPingSetup.exe	02/12/2015	464.09 Kb

Completing the Change MAC Address Setup Wizard

Setup has finished installing Change MAC Address on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch Change MAC Address

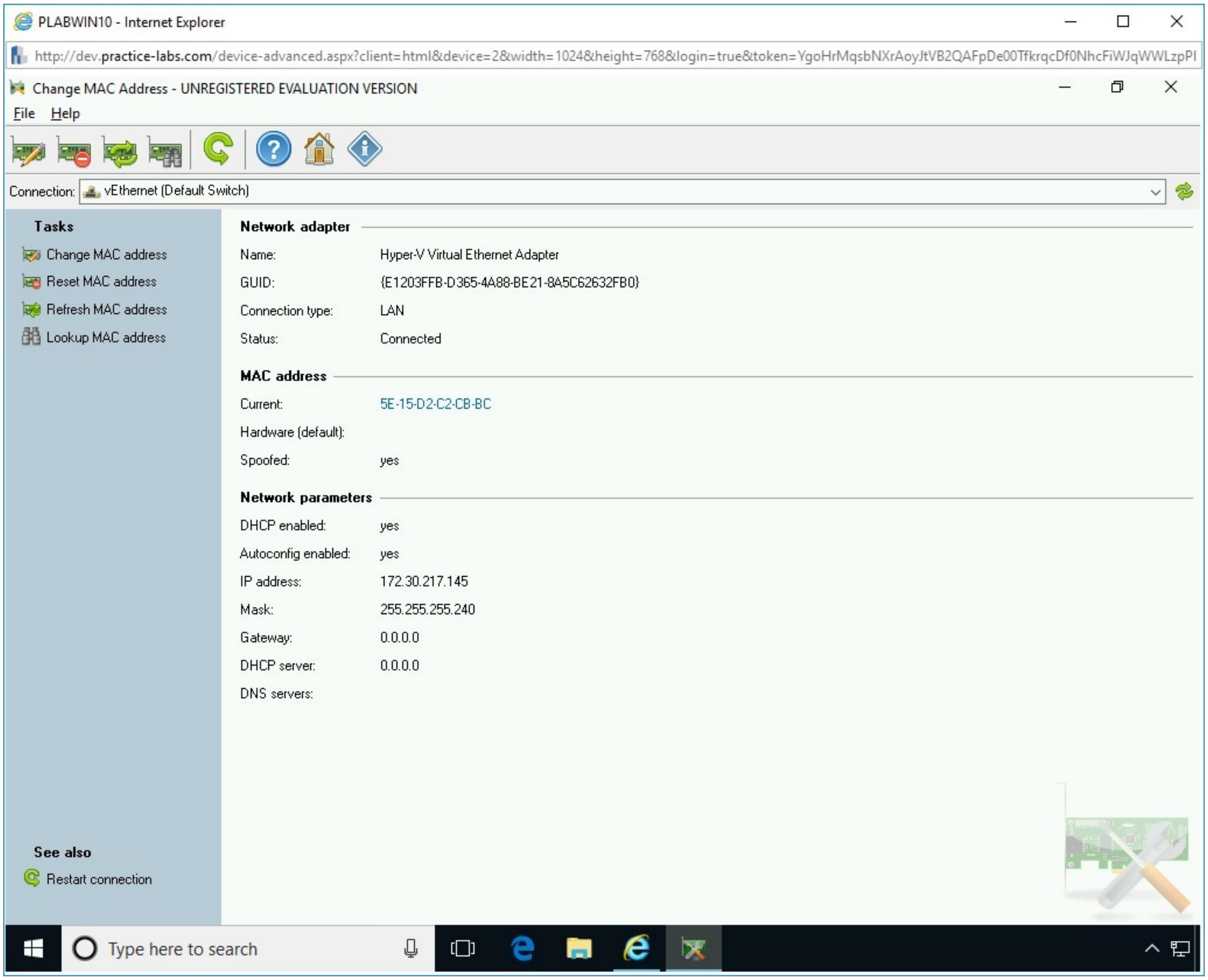
□ Visit Homepage

Figure 1.12 Screenshot of PLABWIN10: Clicking Finish on the installation completion page.

Step 13

Change MAC Address automatically opens after installation.

Minimize **Internet Explorer** and maximize the **Change MAC Address - UNREGISTERED EVALUATION VERSION** window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5E-15-D2-C2-CB-BC

Hardware (default):

Spoofed: yes

Network parameters

DHCP enabled: yes

Autoconfig enabled: yes

IP address: 172.30.217.145

Mask: 255.255.255.240

Gateway: 0.0.0.0

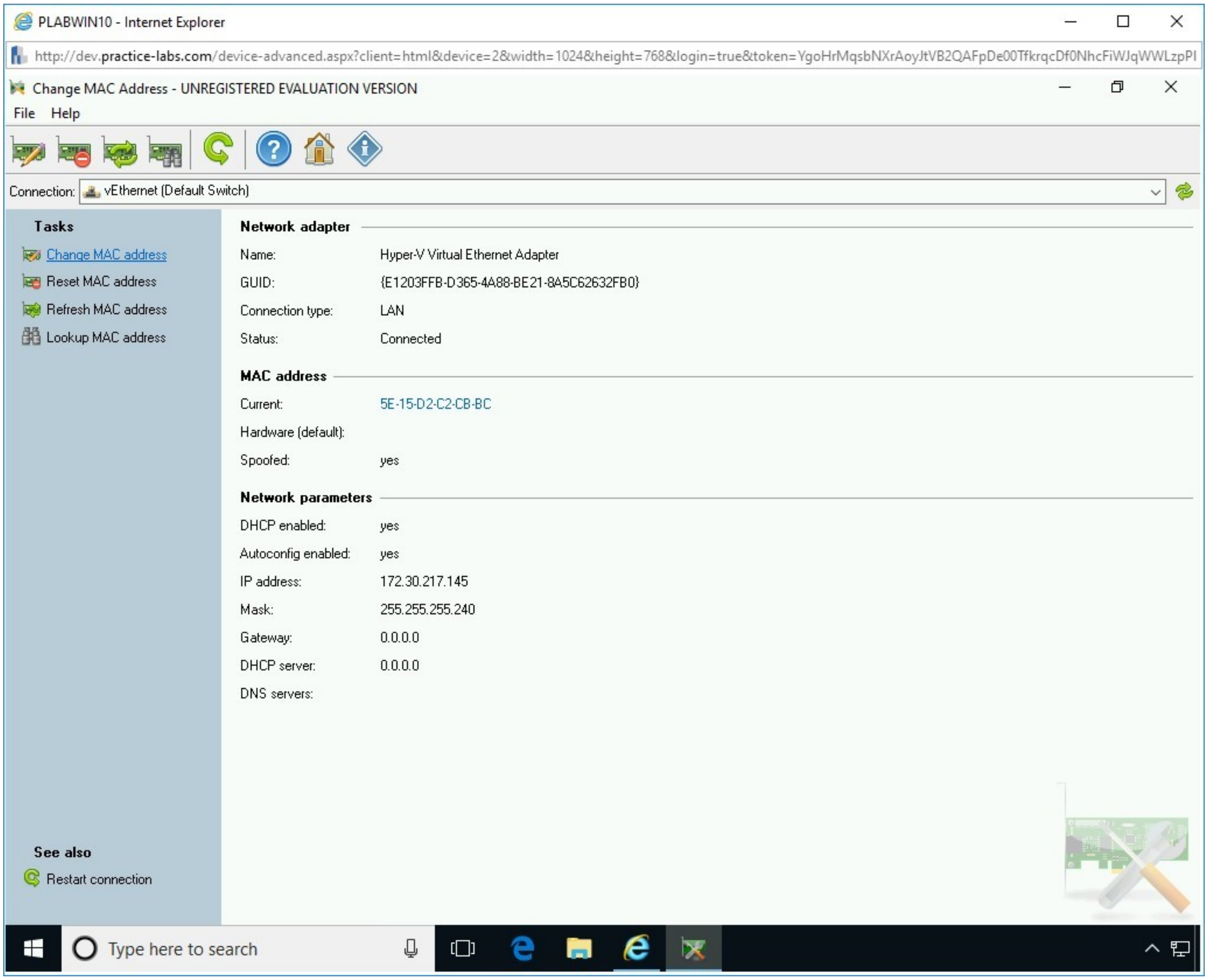
DHCP server: 0.0.0.0

DNS servers:

Figure 1.13 Screenshot of PLABWIN10: Showing the Change MAC Address window.

Step 14

From the left-hand pane, click **Change MAC address**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI

Change MAC Address - UNREGISTERED EVALUATION VERSION

Connection: vEthernet (Default Switch)

Tasks

- Change MAC address
- Reset MAC address
- Refresh MAC address
- Lookup MAC address

See also

- Restart connection

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5E-15-D2-C2-CB-BC

Hardware (default):

Spoofed: yes

Network parameters

DHCP enabled: yes

Autoconfig enabled: yes

IP address: 172.30.217.145

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

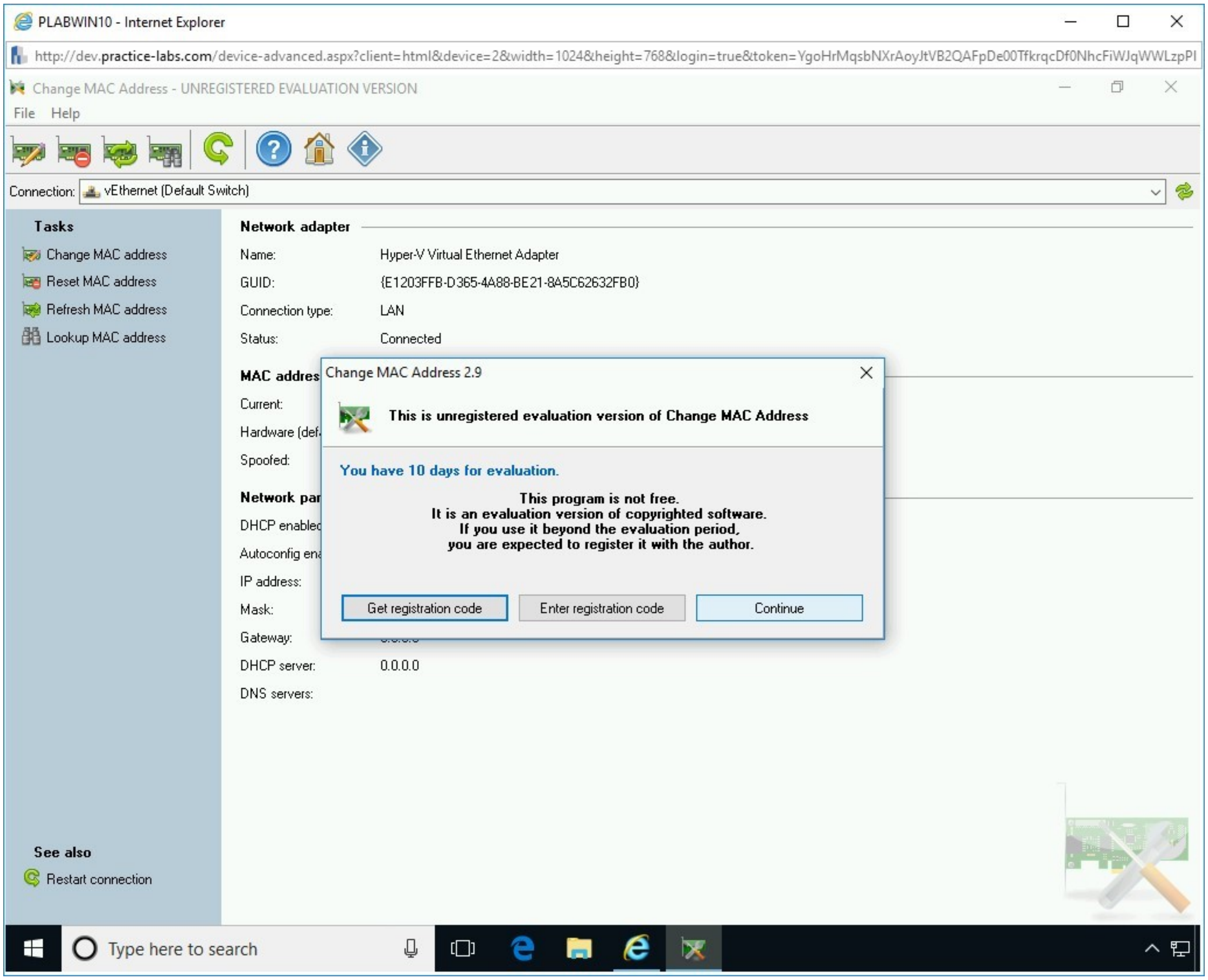
Figure 1.14 Screenshot of PLABWIN10: Clicking Change MAC address in the left-hand pane.

Step 15

The **Change MAC Address 2.9** dialog box is displayed.

> ***Note:*** *This dialog box appears if you are using a trial version. If you enter the registration code for the first time when you open Change MAC Address, this dialog box will no longer appear.*

Click **Continue**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Get registration code
Enter registration code
Continue
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC addres

Current:

Hardware (def

Spoofed:

Network par

DHCP enabled

Autoconfig en

IP address:

Mask:

Gateway:

DHCP server: 0.0.0.0

DNS servers:

Change MAC Address 2.9

This is unregistered evaluation version of Change MAC Address

You have 10 days for evaluation.

This program is not free.
It is an evaluation version of copyrighted software.
If you use it beyond the evaluation period,
you are expected to register it with the author.

Figure 1.15 Screenshot of PLABWIN10: Showing the Change MAC Address 2.9 dialog box and clicking Continue.

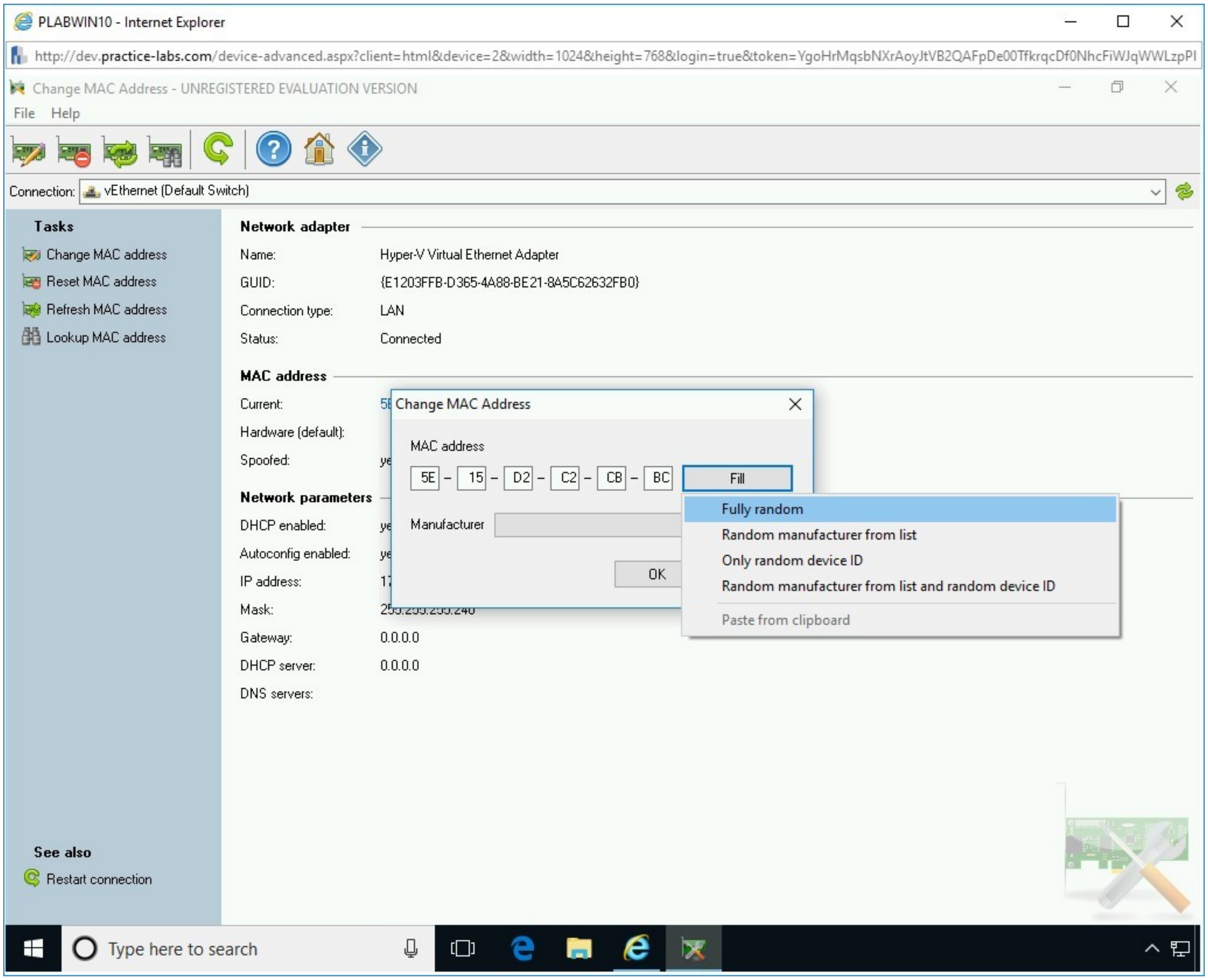
Step 16

The **Change MAC Address** dialog box is displayed.

Note that the MAC address is displayed.

You have multiple options. You can choose to change it randomly, change it with the randomly selected manufacturer, change random device ID, or change with a randomly selected manufacturer with random device ID.

Click **Fill** and select **Fully random**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

Change MAC Address - UNREGISTERED EVALUATION VERSION

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5E

Hardware (default):

Spoofed: ye

Network parameters

DHCP enabled: ye

Autoconfig enabled: ye

IP address: 17

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Change MAC Address

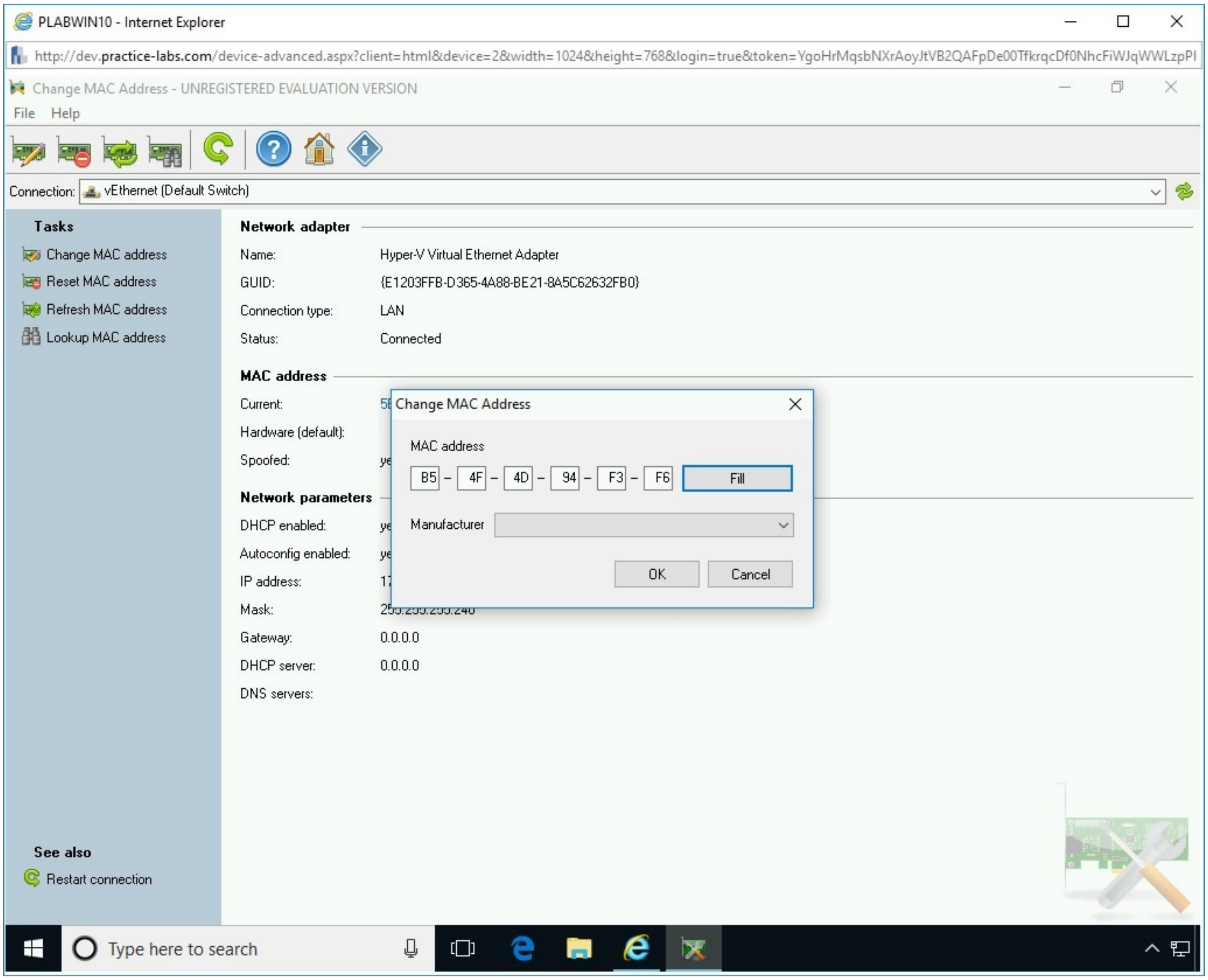
MAC address: 5E - 15 - D2 - C2 - CB - BC

Manufacturer

Figure 1.16 Screenshot of PLABWIN10: Clicking Fill on the Change MAC Address dialog box and selecting Fully random.

Step 17

The **MAC** address has now changed.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI

Change MAC Address - UNREGISTERED EVALUATION VERSION

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5

Hardware (default):

Spoofed: ye

Network parameters

DHCP enabled: ye

Autoconfig enabled: ye

IP address: 1

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Change MAC Address

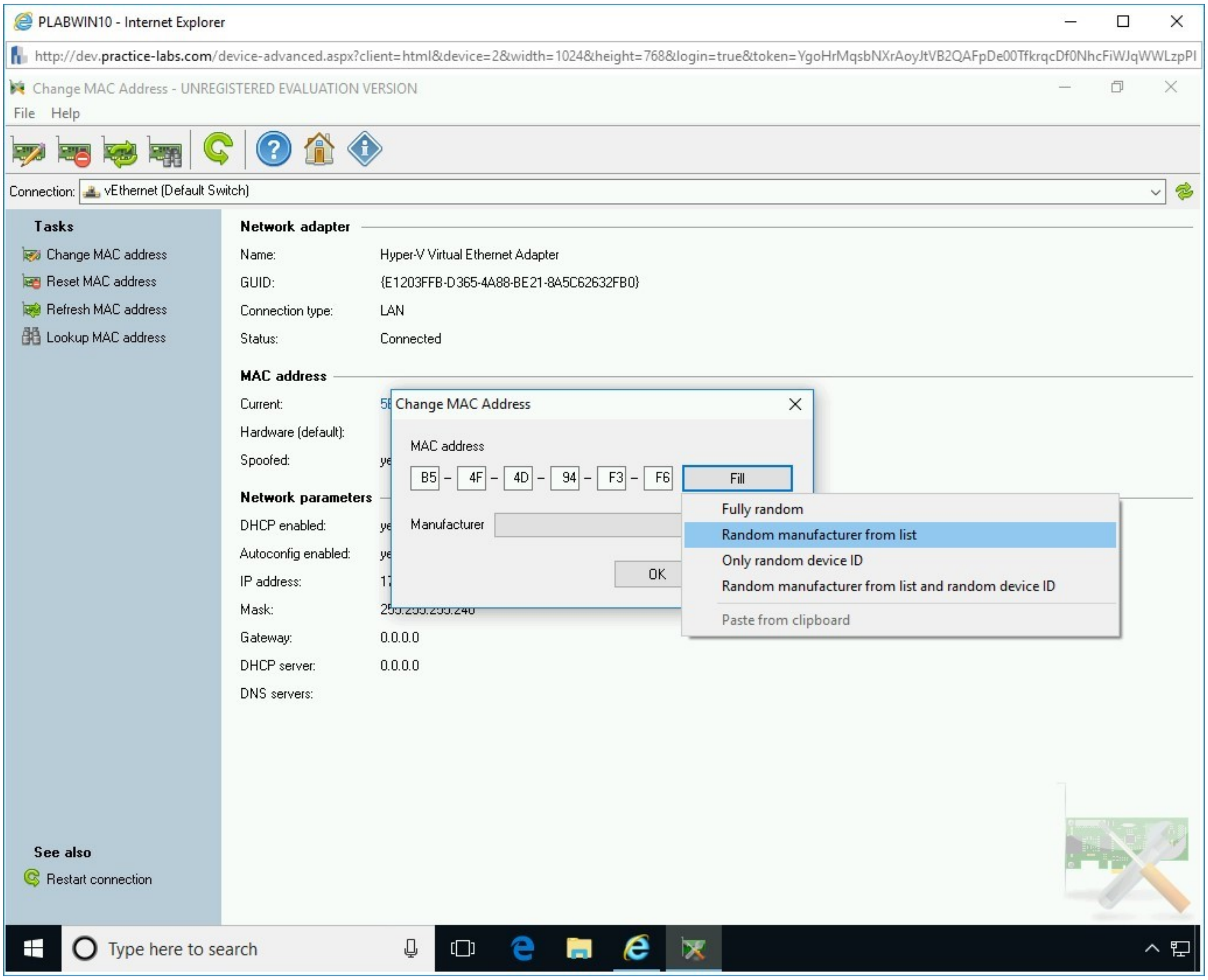
MAC address B5 – 4F – 4D – 94 – F3 – F6

Manufacturer

Figure 1.17 Screenshot of PLABWIN10: Showing the changed MAC address in the Change MAC Address dialog box.

Step 18

Click **Fill** and select **Random manufacturer from list**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter
GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}
Connection type: LAN
Status: Connected

MAC address

Current: 5E
Hardware (default):
Spoofed: ye

Network parameters

DHCP enabled: ye
Autoconfig enabled: ye
IP address: 17
Mask: 255.255.255.240
Gateway: 0.0.0.0
DHCP server: 0.0.0.0
DNS servers:

Change MAC Address

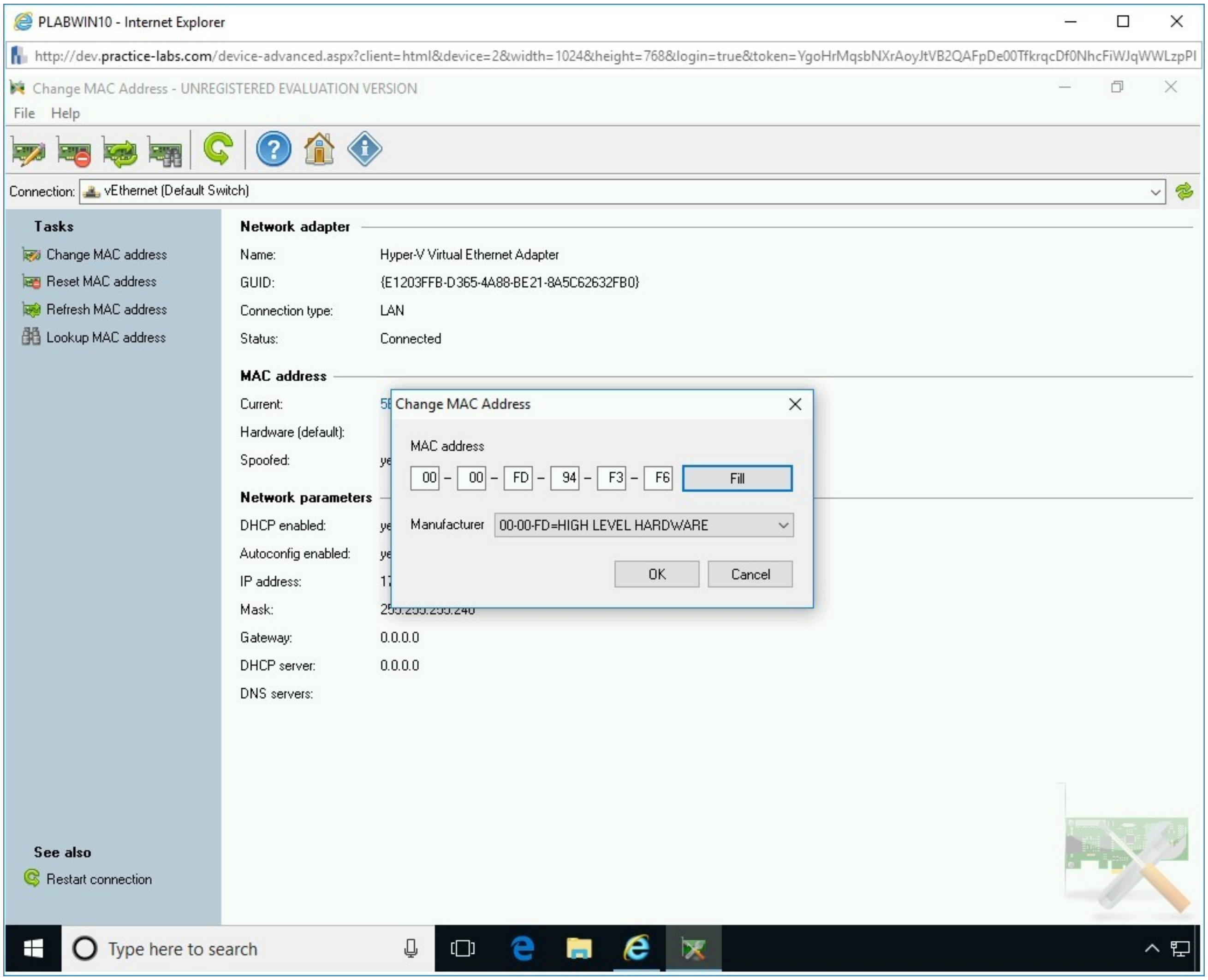
MAC address
B5 – 4F – 4D – 94 – F3 – F6

Manufacturer

Figure 1.18 Screenshot of PLABWIN10: Clicking Fill and selecting Random manufacturer from the drop-down list on the Change MAC Address dialog box.

Step 19

Note that both the **MAC address** and **Manufacturer** are changed.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

Change MAC Address - UNREGISTERED EVALUATION VERSION

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5E

Hardware (default):

Spoofed: ye

Network parameters

DHCP enabled: ye

Autoconfig enabled: ye

IP address: 17

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Change MAC Address

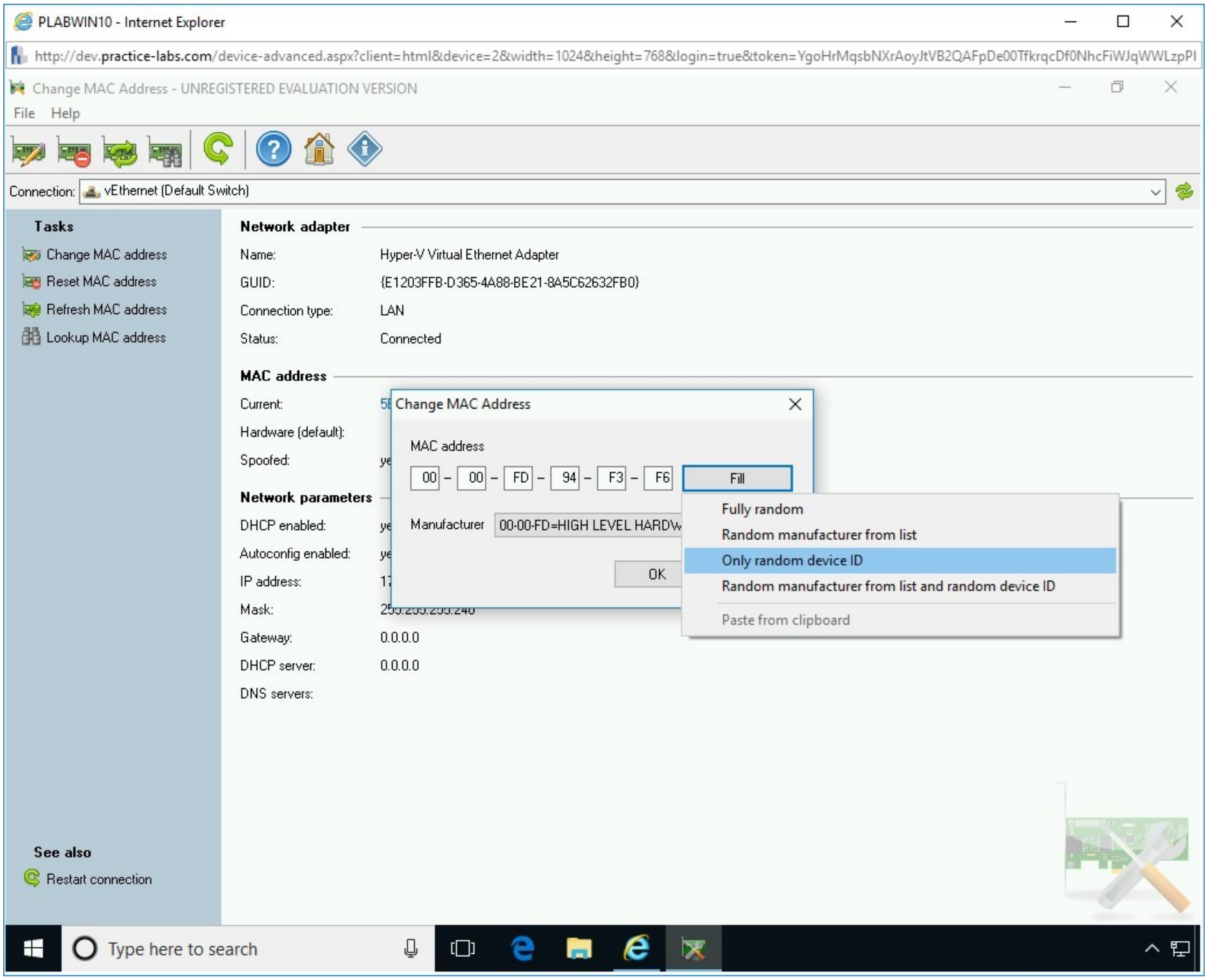
MAC address: 00 – 00 – FD – 94 – F3 – F6

Manufacturer: 00-00-FD=HIGH LEVEL HARDWARE

Figure 1.19 Screenshot of PLABWIN10: Showing the changed MAC address and manufacturer in the Change MAC Address dialog box.

Step 10

Click **Fill** and select **Only random device ID**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Change MAC Address
Fill
Fully random
Random manufacturer from list
Only random device ID
Random manufacturer from list and random device ID
Paste from clipboard
OK
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5E

Hardware (default):

Spoofed: ye

Network parameters

DHCP enabled: ye

Autoconfig enabled: ye

IP address: 17

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

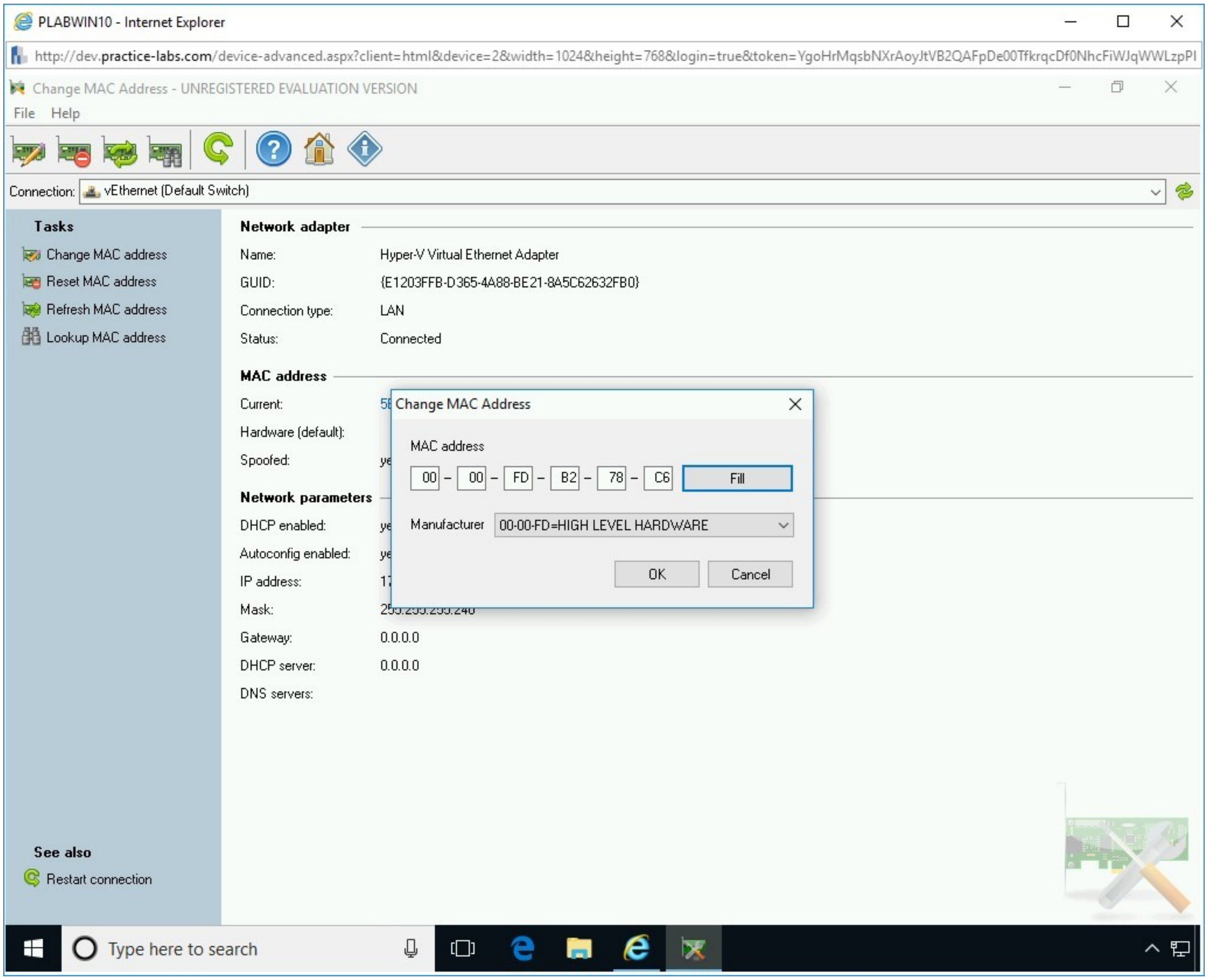
MAC address: 00 – 00 – FD – 94 – F3 – F6

Manufacturer: 00-00-FD=HIGH LEVEL HARDW

Figure 1.20 Screenshot of PLABWIN10: Clicking Fill and selecting Only random device ID on the drop-down list on the Change MAC Address dialog box.

Step 21

Note that the **MAC address** is changed.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5

Hardware (default):

Spoofed: ye

Network parameters

DHCP enabled: ye

Autoconfig enabled: ye

IP address: 17

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Change MAC Address

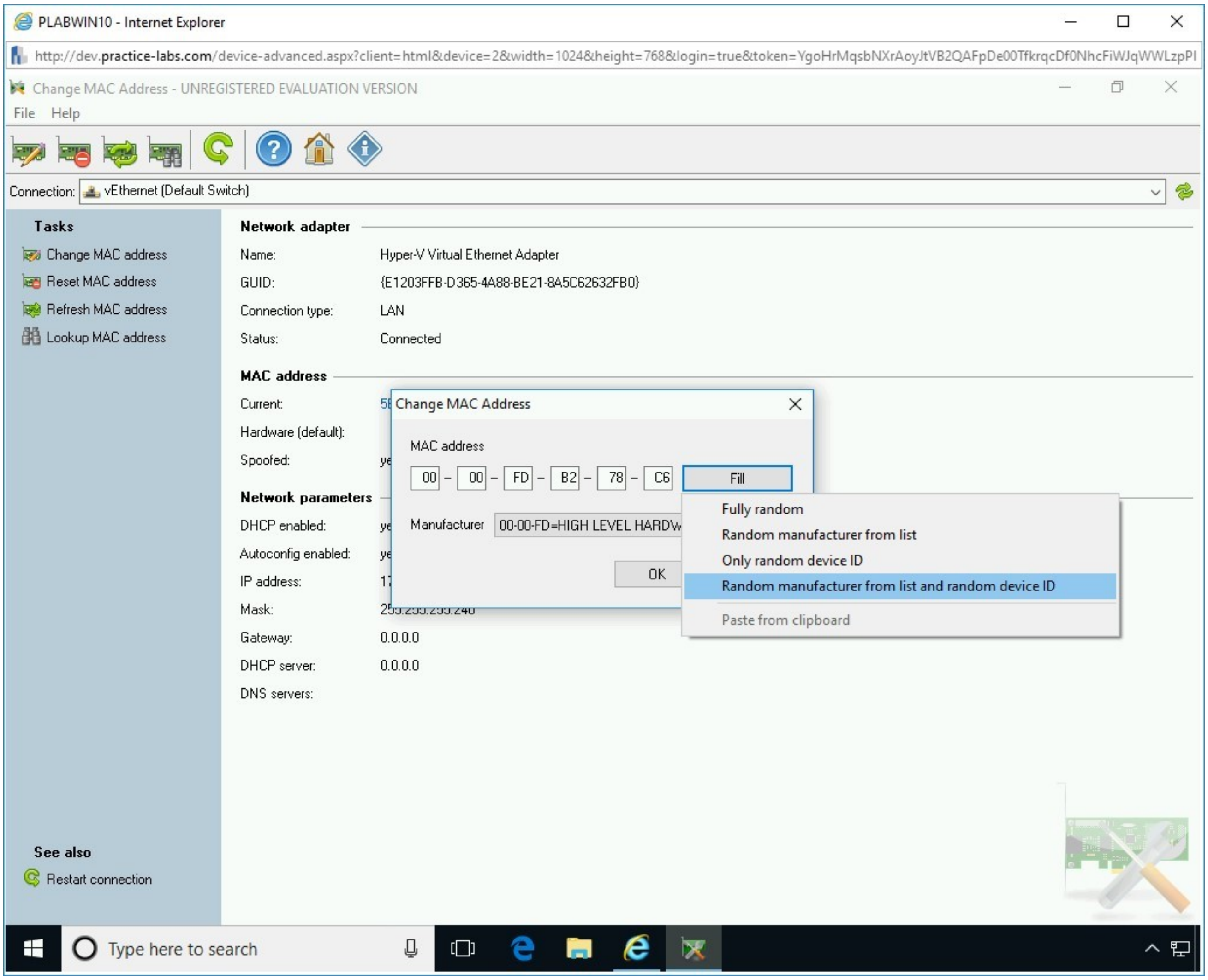
MAC address: 00 - 00 - FD - B2 - 78 - C6

Manufacturer: 00-00-FD=HIGH LEVEL HARDWARE

Figure 1.21 Screenshot of PLABWIN10: Showing the changed MAC address in the Change MAC Address dialog box

Step 22

Click **Fill** and select **Random manufacturer from list and random device ID**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Fill
Fully random
Random manufacturer from list
Only random device ID
Random manufacturer from list and random device ID
Paste from clipboard
OK
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5

Hardware (default):

Spoofed: ye

Network parameters

DHCP enabled: ye

Autoconfig enabled: ye

IP address: 17

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Change MAC Address

MAC address

00 – 00 – FD – B2 – 78 – C6

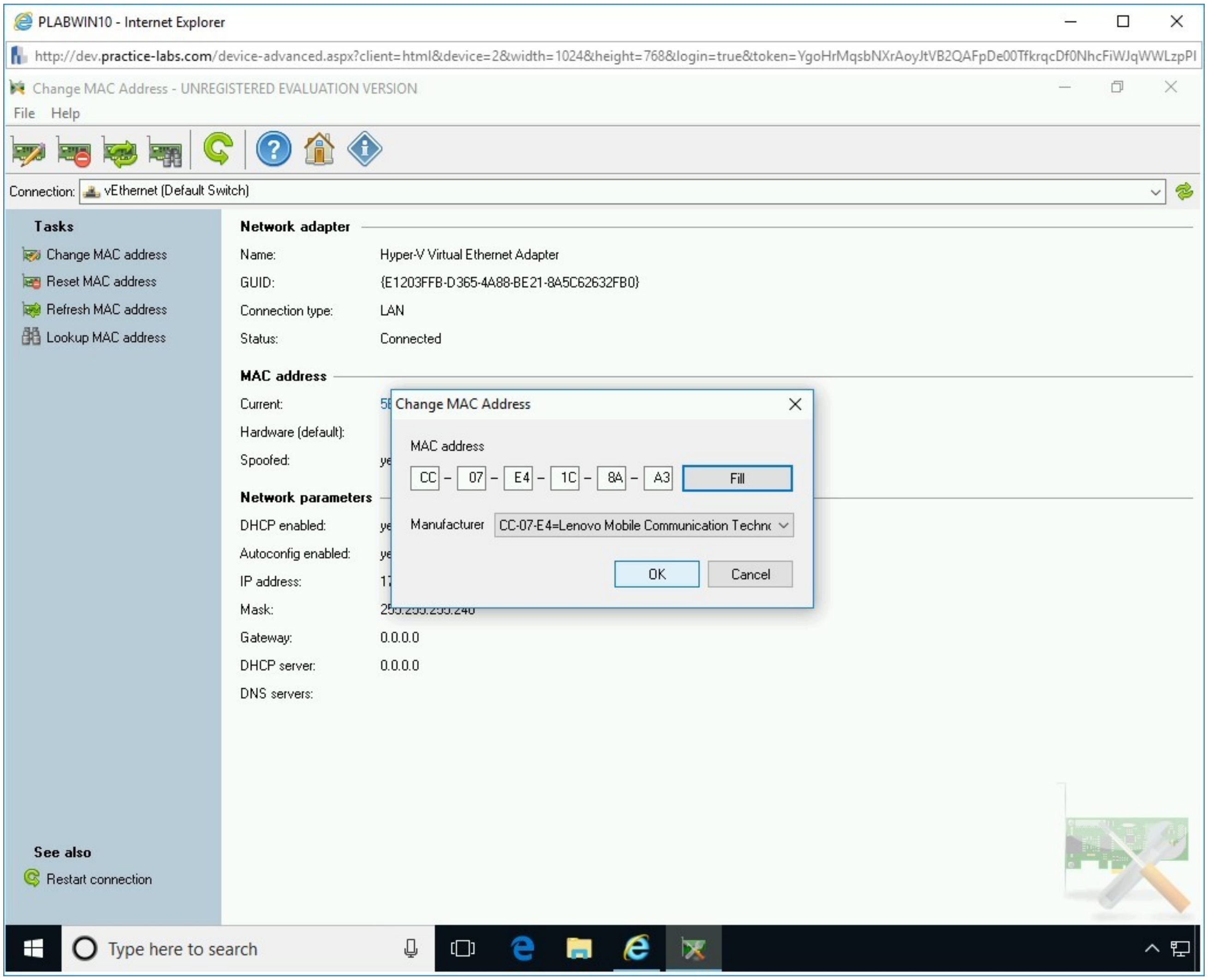
Manufacturer 00-00-FD=HIGH LEVEL HARDW

Figure 1.22 Screenshot of PLABWIN10: Clicking Fill and selecting Random manufacturer from list and random device ID on the Change MAC Address dialog box.

Step 23

Note that both have changed.

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter
GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}
Connection type: LAN
Status: Connected

MAC address

Current: 5E
Hardware (default):
Spoofed: ye

Network parameters

DHCP enabled: ye
Autoconfig enabled: ye
IP address: 17
Mask: 255.255.255.240
Gateway: 0.0.0.0
DHCP server: 0.0.0.0
DNS servers:

Change MAC Address

MAC address: CC - 07 - E4 - 1C - 8A - A3 [Fill]

Manufacturer: CC-07-E4=Lenovo Mobile Communication Techn

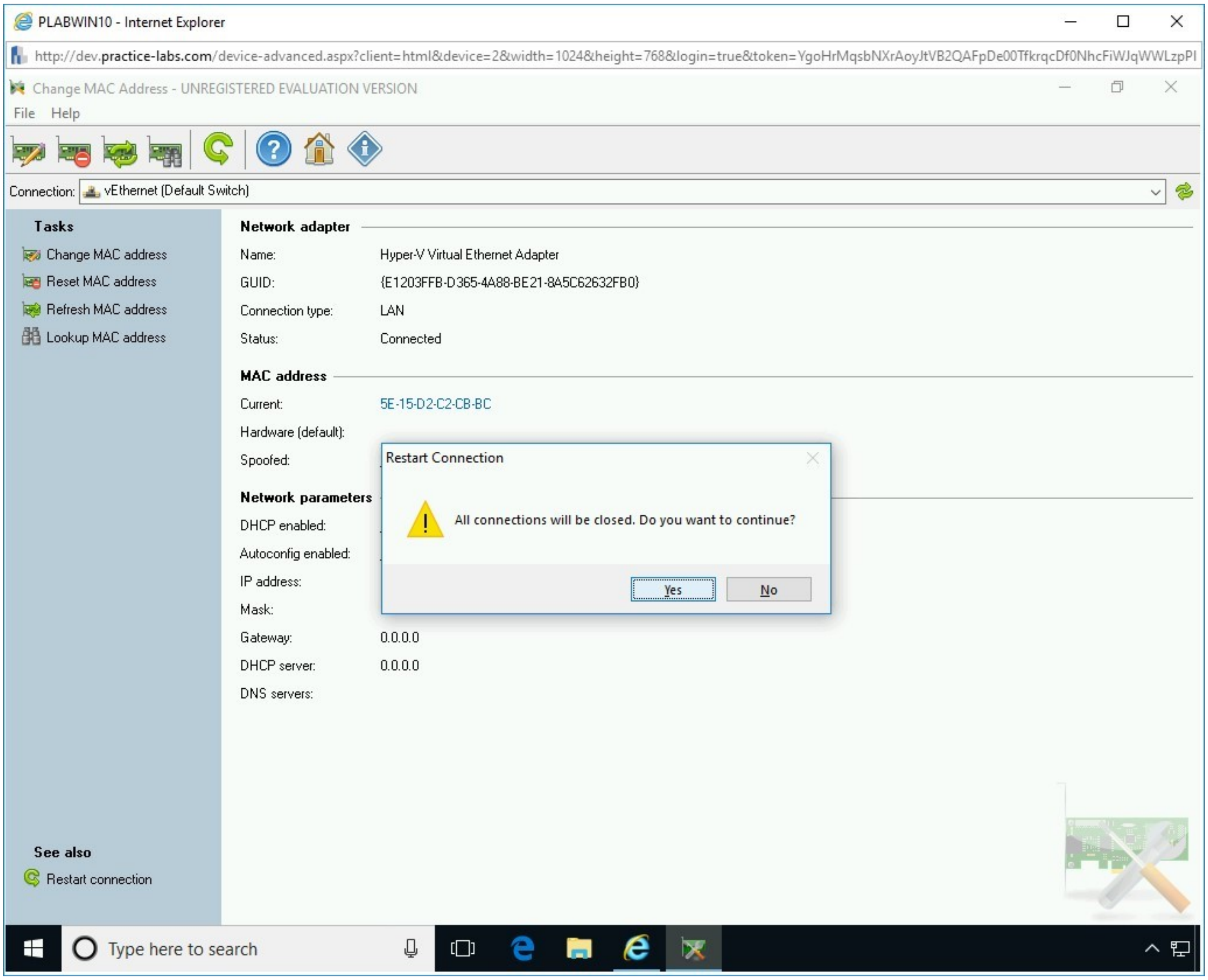
[OK] [Cancel]

Figure 1.23 Screenshot of PLABWIN10: Showing the changed MAC address and manufacturer on the Change MAC Address dialog box and clicking OK.

Step 24

The **Restart Connection** dialog box is displayed. It prompts you to restart the connection to allow the new MAC address to change effect.

Click **Yes**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Type here to search

Connection: vEthernet (Default Switch)

Tasks

- Change MAC address
- Reset MAC address
- Refresh MAC address
- Lookup MAC address

See also

- Restart connection

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: 5E-15-D2-C2-CB-BC

Hardware (default):

Spoofed:

Network parameters

DHCP enabled:

Autoconfig enabled:

IP address:

Mask:

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Restart Connection

All connections will be closed. Do you want to continue?

Yes No

Figure 1.24 Screenshot of PLABWIN10: Clicking Yes to restart the system.

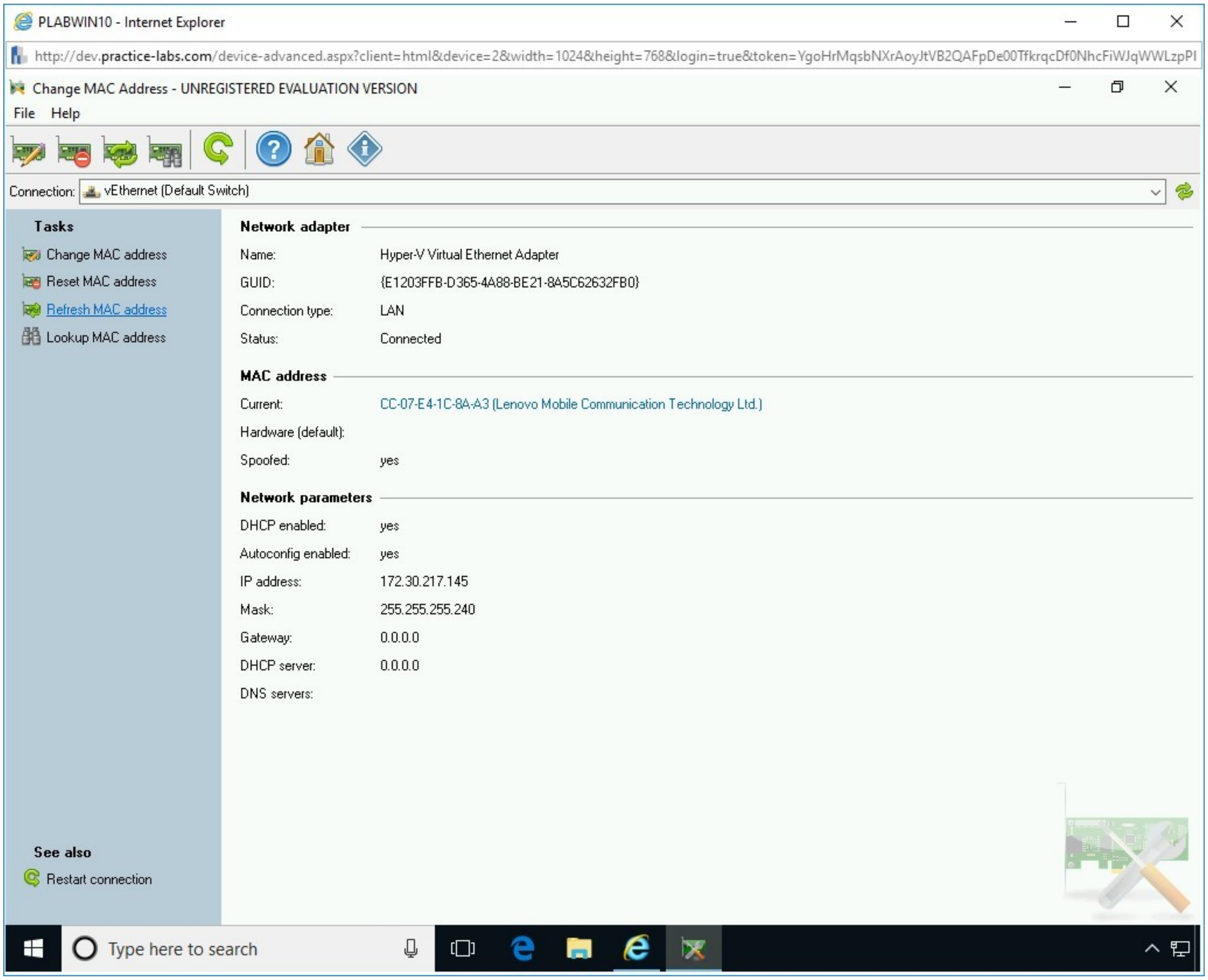
Step 25

The **Configuration Interface** dialog box is displayed.

It shows that the disconnecting is in process.

In the left-hand pane, click **Refresh MAC address**.

Note that the right-hand pane now displays the updated address along with the manufacturer.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter
GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}
Connection type: LAN
Status: Connected

MAC address

Current: CC-07-E4-1C-8A-A3 (Lenovo Mobile Communication Technology Ltd.)
Hardware (default):
Spoofed: yes

Network parameters

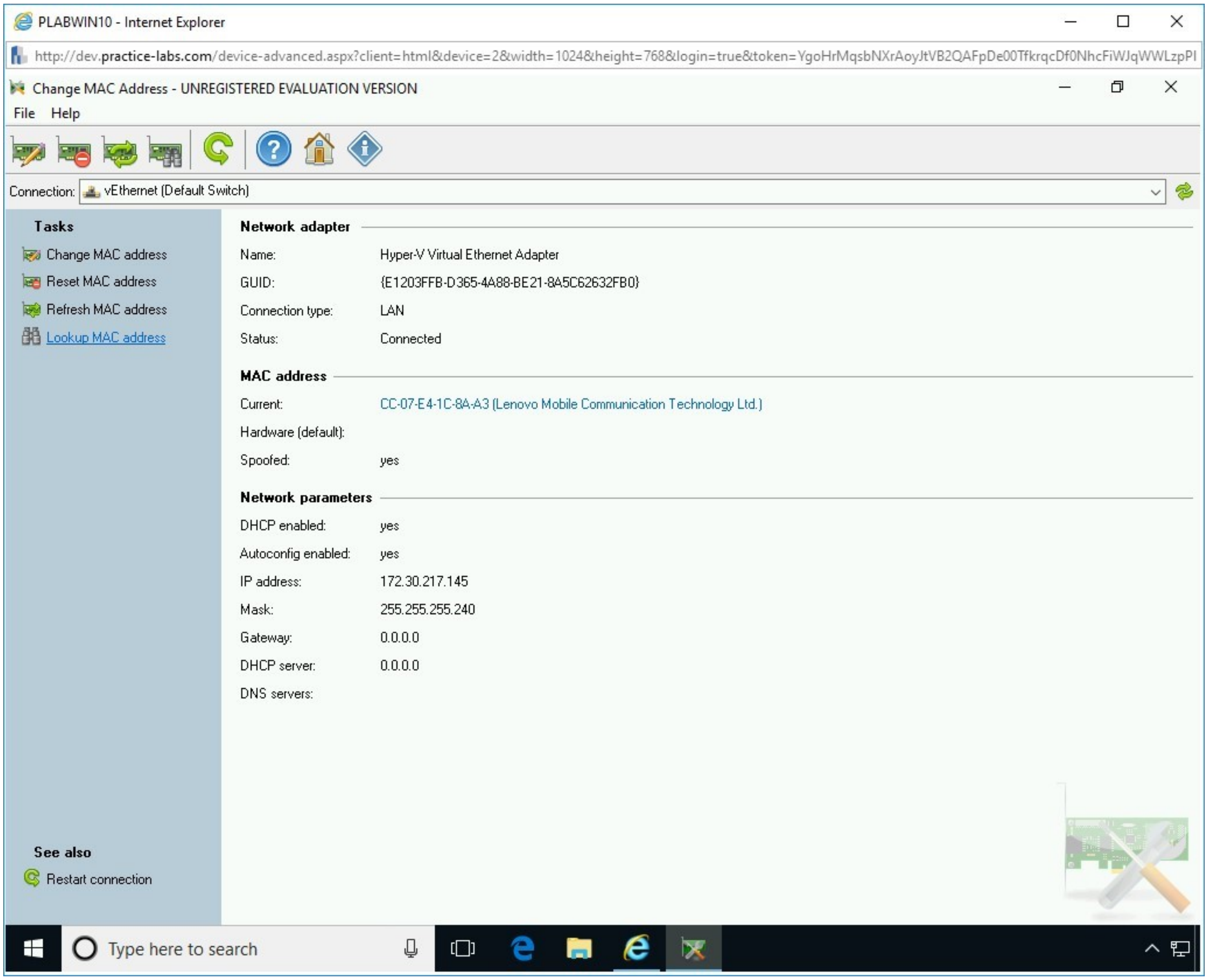
DHCP enabled: yes
Autoconfig enabled: yes
IP address: 172.30.217.145
Mask: 255.255.255.240
Gateway: 0.0.0.0
DHCP server: 0.0.0.0
DNS servers:

Figure 1.25 Screenshot of PLABWIN10: Clicking Refresh MAC address in the left-hand pane.

Step 26

You can also identify the manufacturer based on an identified **MAC** address.

From the left-hand pane, click **Lookup MAC address**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Connection:
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current: CC-07-E4-1C-8A-A3 (Lenovo Mobile Communication Technology Ltd.)

Hardware (default):

Spoofed: yes

Network parameters

DHCP enabled: yes

Autoconfig enabled: yes

IP address: 172.30.217.145

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

Figure 1.26 Screenshot of PLABWIN10: Clicking Lookup MAC address in the left-hand pane.

Step 27

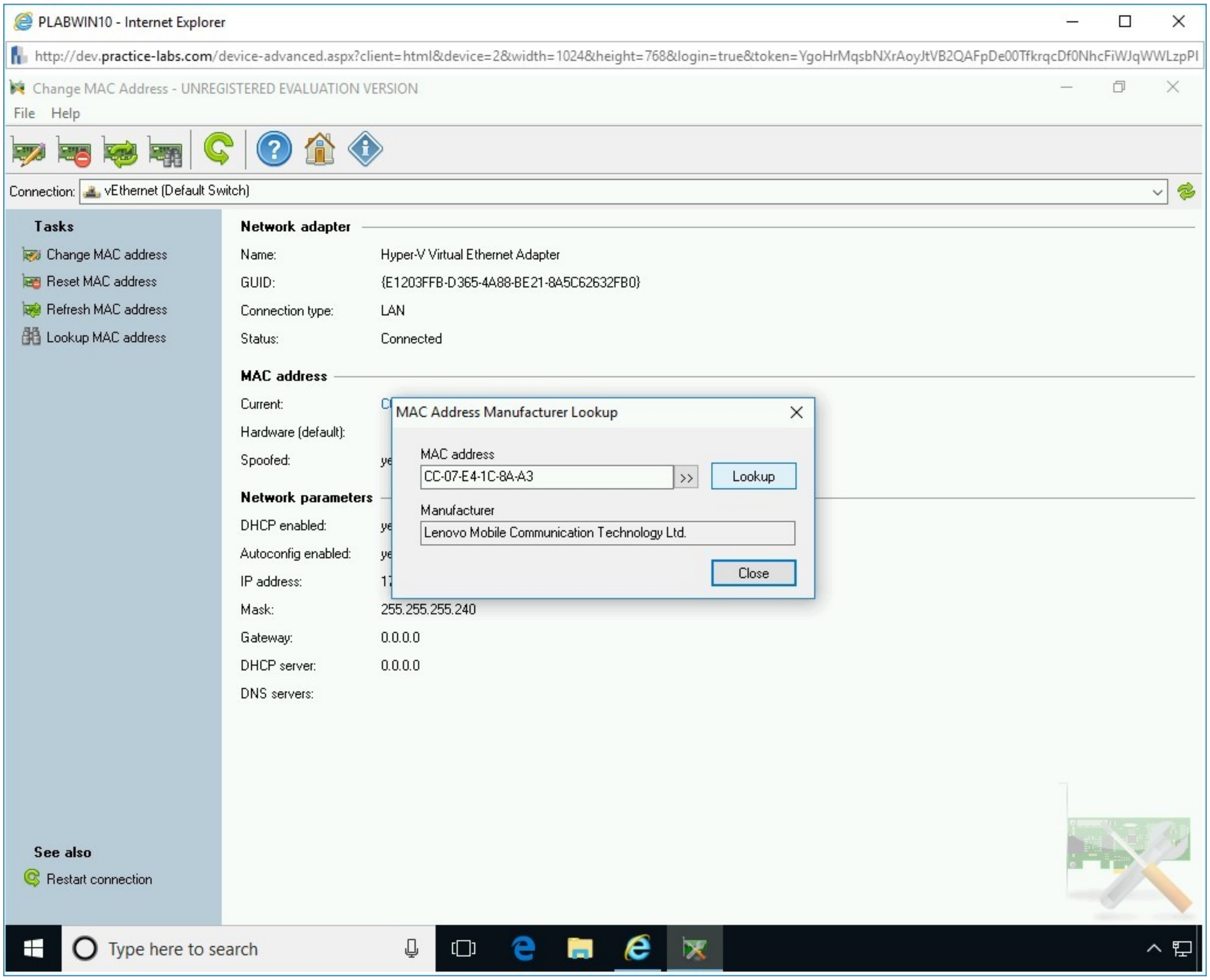
The **MAC Address Manufacturer Lookup** dialog box is displayed.

> ***Note***: *You may get different values compared to the screenshot.*

In the **MAC address** textbox, change the MAC address generated in the previous step to a new MAC address.

Click **Lookup**.

Note: *The Lookup option works if the Manufacturer's name does not appear in the Manufacturer drop-down. In the lab, the manufacturer's name is already visible, and therefore, there will be no change in the name.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter

GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}

Connection type: LAN

Status: Connected

MAC address

Current:

Hardware (default):

Spoofed:

Network parameters

DHCP enabled:

Autoconfig enabled:

IP address:

Mask: 255.255.255.240

Gateway: 0.0.0.0

DHCP server: 0.0.0.0

DNS servers:

MAC Address Manufacturer Lookup

MAC address: CC-07-E4-1C-8A-A3 [>>] [Lookup]

Manufacturer: Lenovo Mobile Communication Technology Ltd.

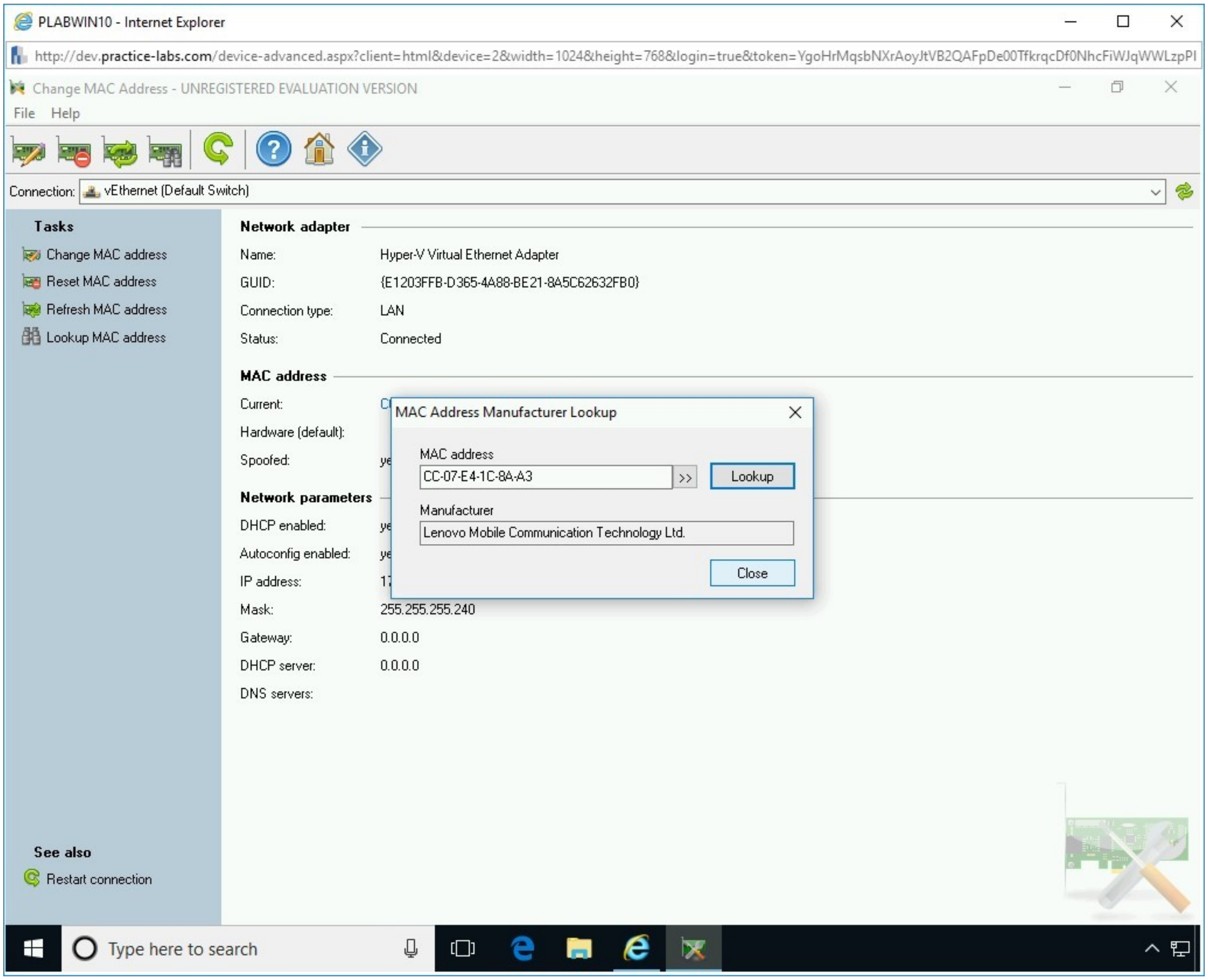
[Close]

Figure 1.27 Screenshot of PLABWIN10: Clicking Lookup on the MAC Address Manufacturer Lookup dialog box.

Step 28

Note that the name of the manufacturer does not change in the **Manufacturer** textbox.

Click **Close** & exit from the **Change MAC Address** tool.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Change MAC Address - UNREGISTERED EVALUATION VERSION
File
Help
Tasks
Change MAC address
Reset MAC address
Refresh MAC address
Lookup MAC address
See also
Restart connection
Lookup
Close
Type here to search

Connection: vEthernet (Default Switch)

Network adapter

Name: Hyper-V Virtual Ethernet Adapter
GUID: {E1203FFB-D365-4A88-BE21-8A5C62632FB0}
Connection type: LAN
Status: Connected

MAC address

Current: C
Hardware (default):
Spoofed: ye

Network parameters

DHCP enabled: ye
Autoconfig enabled: ye
IP address: 17
Mask: 255.255.255.240
Gateway: 0.0.0.0
DHCP server: 0.0.0.0
DNS servers:

MAC Address Manufacturer Lookup

MAC address: CC-07-E4-1C-8A-A3
Manufacturer: Lenovo Mobile Communication Technology Ltd.

Figure 1.28 Screenshot of PLABWIN10: Clicking Close on the MAC Address Manufacturer Lookup dialog box.

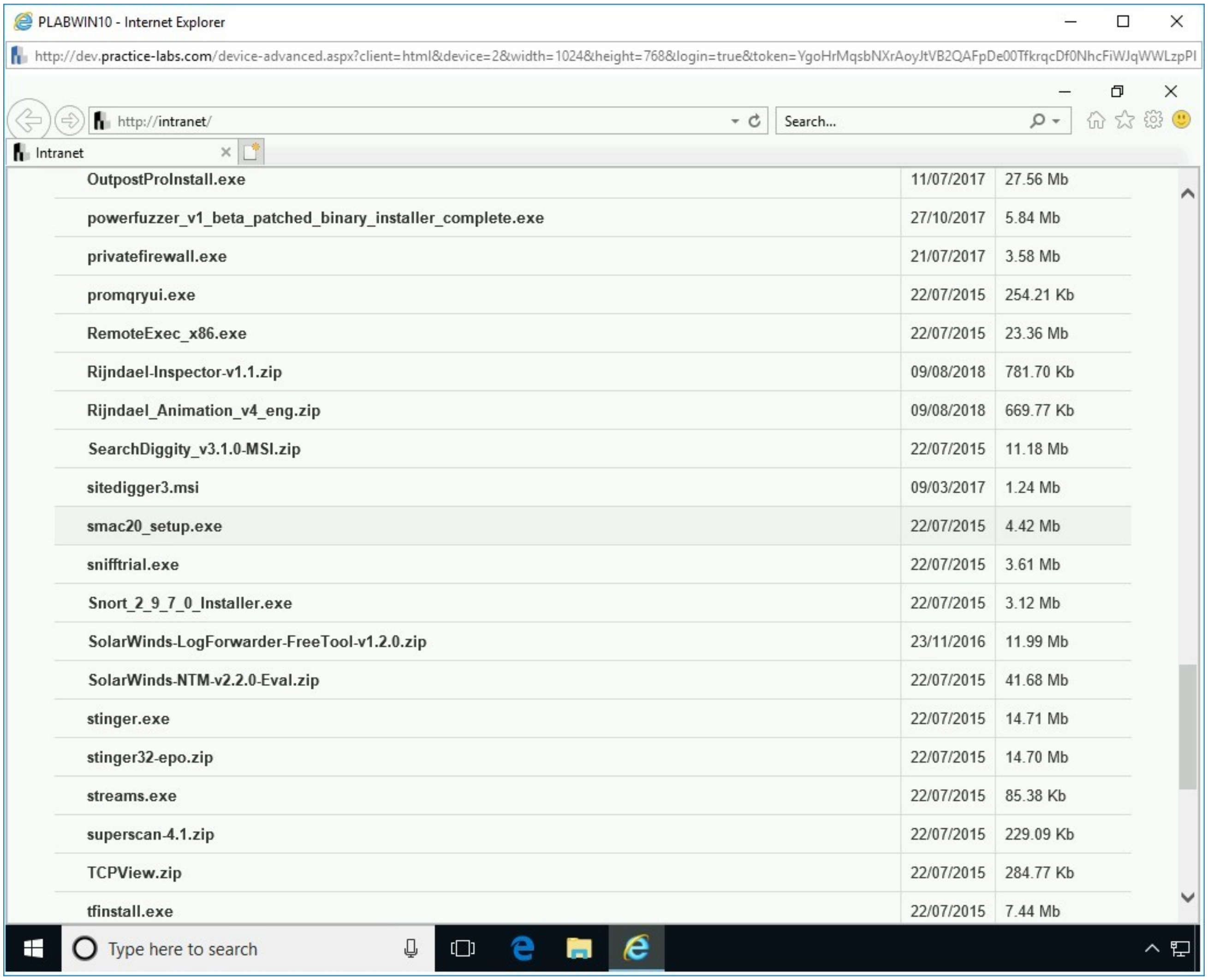
Task 2 - Use SMAC 2.0

SMAC is a **MAC** spoofing application, which means that it can change the **MAC** address.

In this task, you will learn to use **SMAC**. To use **SMAC**, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**. Restore Internet Explorer from the taskbar. You should be on the Hacking Tools page. Locate **smac20_setup.exe**, and then click on it.

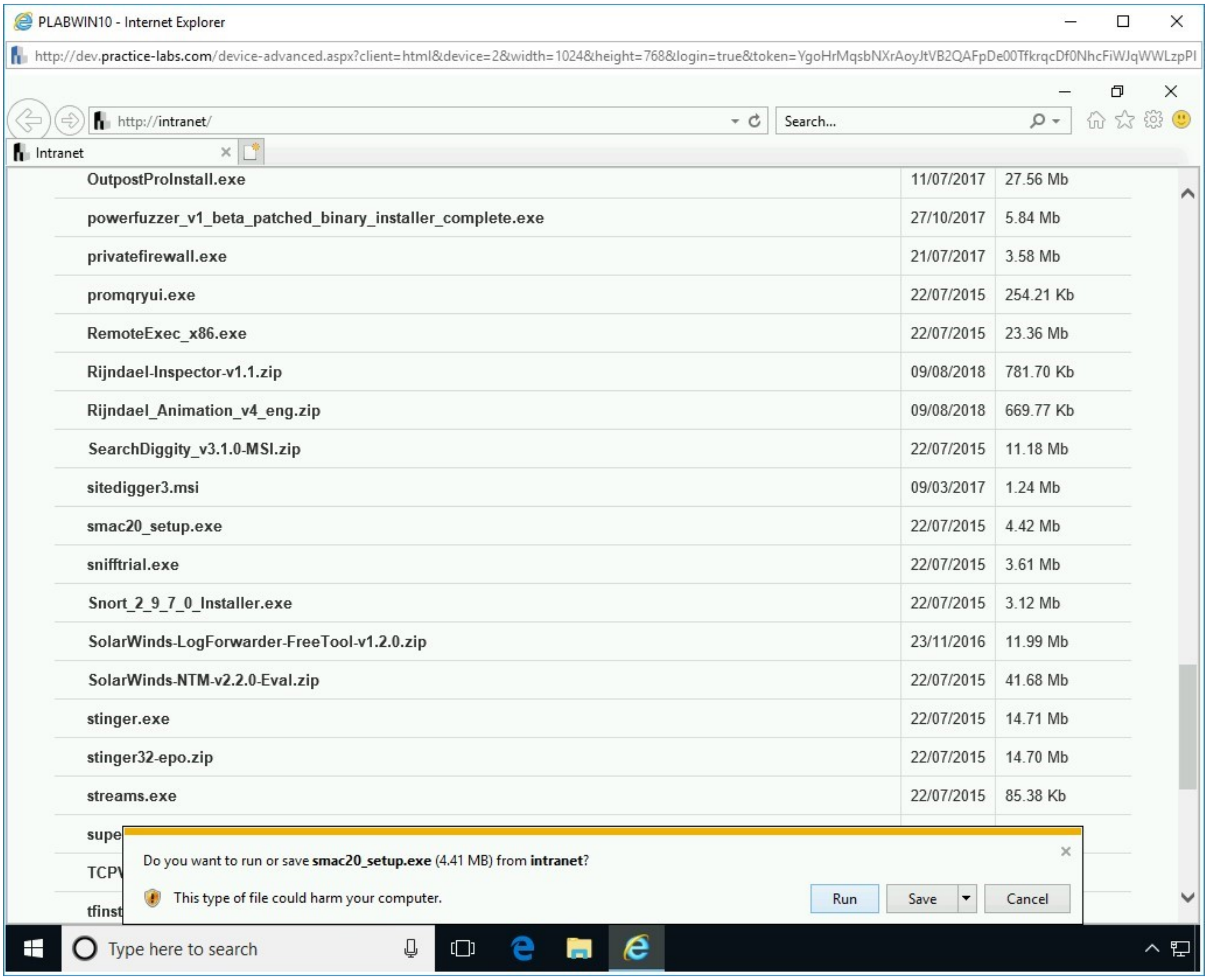

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Type here to search

OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb

Figure 1.29 Screenshot of PLABWIN10: Internet Explorer Intranet page displayed. Clicking smac20_setup.exe to download it.

Step 2

In the notification bar, click **Run**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
Type here to search

OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
supe		
TCPV		
tfinst		

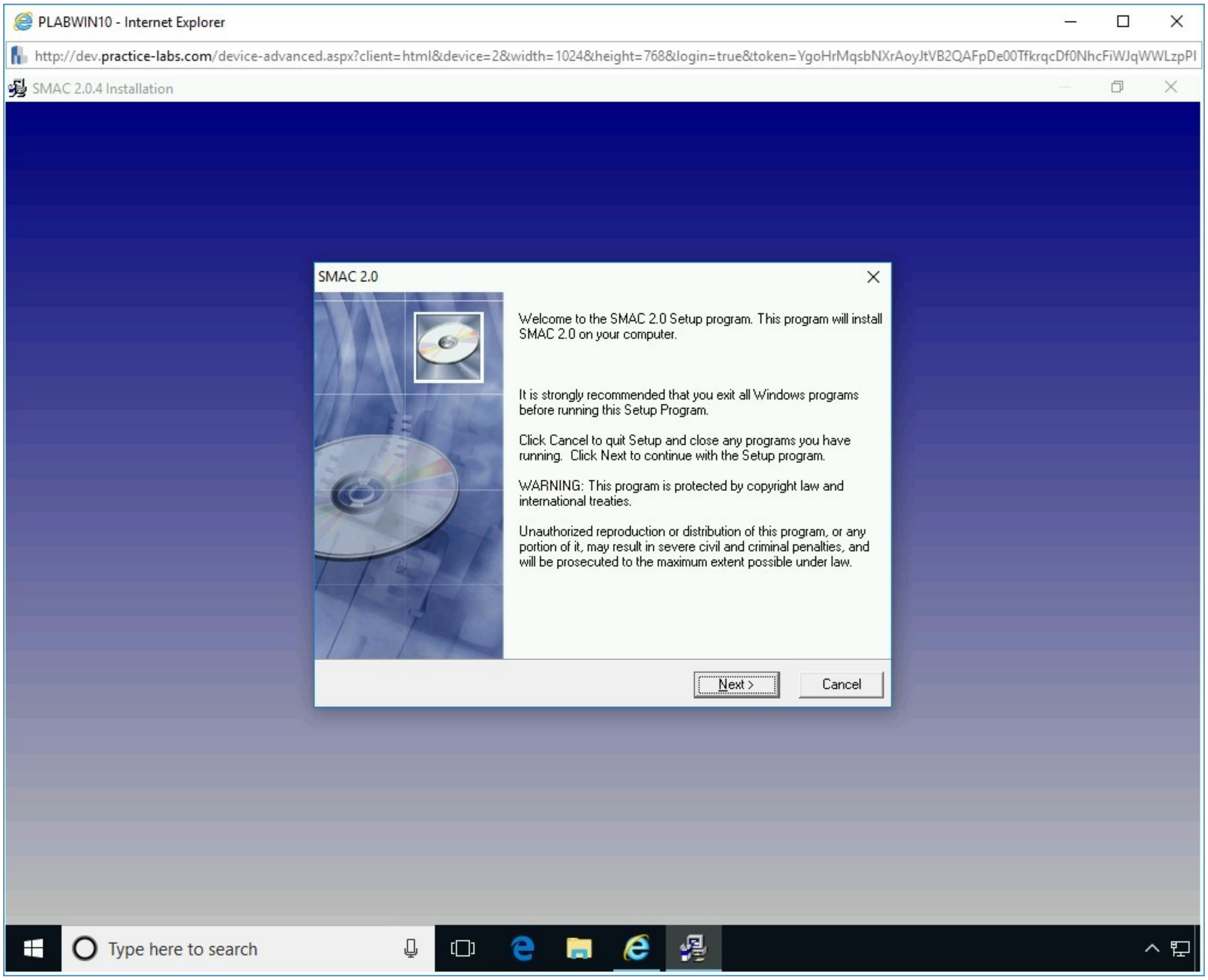
Do you want to run or save **smac20_setup.exe** (4.41 MB) from **intranet**?

This type of file could harm your computer.

Figure 1.30 Screenshot of PLABWIN10: Clicking Run on the notification bar.

Step 3

The **SMAC 2.04 Installation** wizard appears. On the welcome page, click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
SMAC 2.0.4 Installation
SMAC 2.0
Next >
Cancel
Type here to search

Welcome to the SMAC 2.0 Setup program. This program will install SMAC 2.0 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup Program.

Click Cancel to quit Setup and close any programs you have running. Click Next to continue with the Setup program.

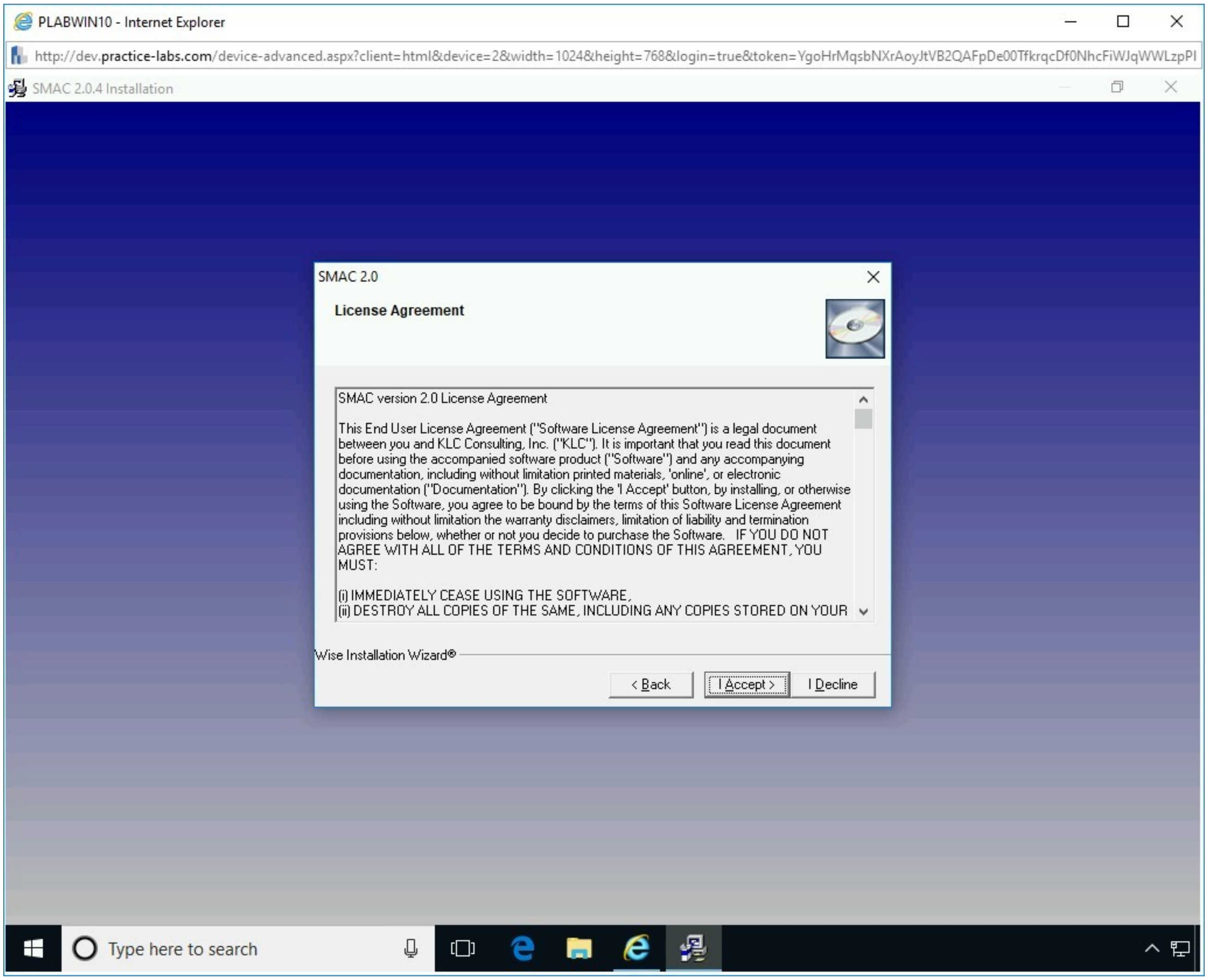
WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 1.31 Screenshot of PLABWIN10: Showing the welcome page of the installation wizard. Clicking Next.

Step 4

On the **License Agreement** page, click **I Accept**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
SMAC 2.0.4 Installation
SMAC 2.0
License Agreement
Wise Installation Wizard®
< Back
I Accept >
I Decline
Type here to search

SMAC version 2.0 License Agreement

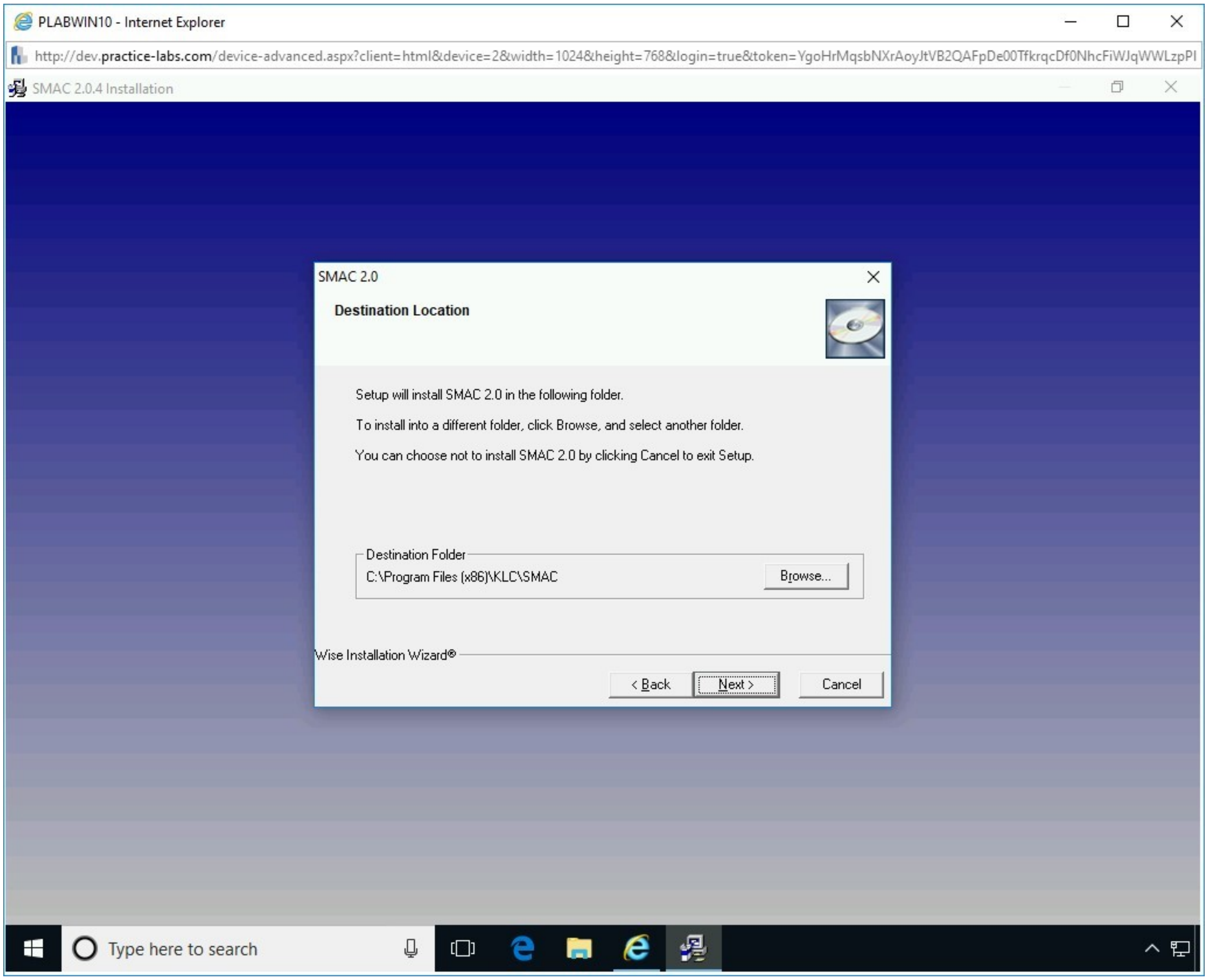
This End User License Agreement ("Software License Agreement") is a legal document between you and KLC Consulting, Inc. ("KLC"). It is important that you read this document before using the accompanied software product ("Software") and any accompanying documentation, including without limitation printed materials, 'online', or electronic documentation ("Documentation"). By clicking the 'I Accept' button, by installing, or otherwise using the Software, you agree to be bound by the terms of this Software License Agreement including without limitation the warranty disclaimers, limitation of liability and termination provisions below, whether or not you decide to purchase the Software. IF YOU DO NOT AGREE WITH ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU MUST:

(i) IMMEDIATELY CEASE USING THE SOFTWARE,
(ii) DESTROY ALL COPIES OF THE SAME, INCLUDING ANY COPIES STORED ON YOUR

Figure 1.32 Screenshot of PLABWIN10: Clicking I Accept on the License Agreement page and clicking Next.

Step 5

On the **Destination Location** page, keep the default location and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
SMAC 2.0.4 Installation
SMAC 2.0
Wise Installation Wizard®
< Back
Next >
Cancel
Browse...
Type here to search

Destination Location

Setup will install SMAC 2.0 in the following folder.

To install into a different folder, click Browse, and select another folder.

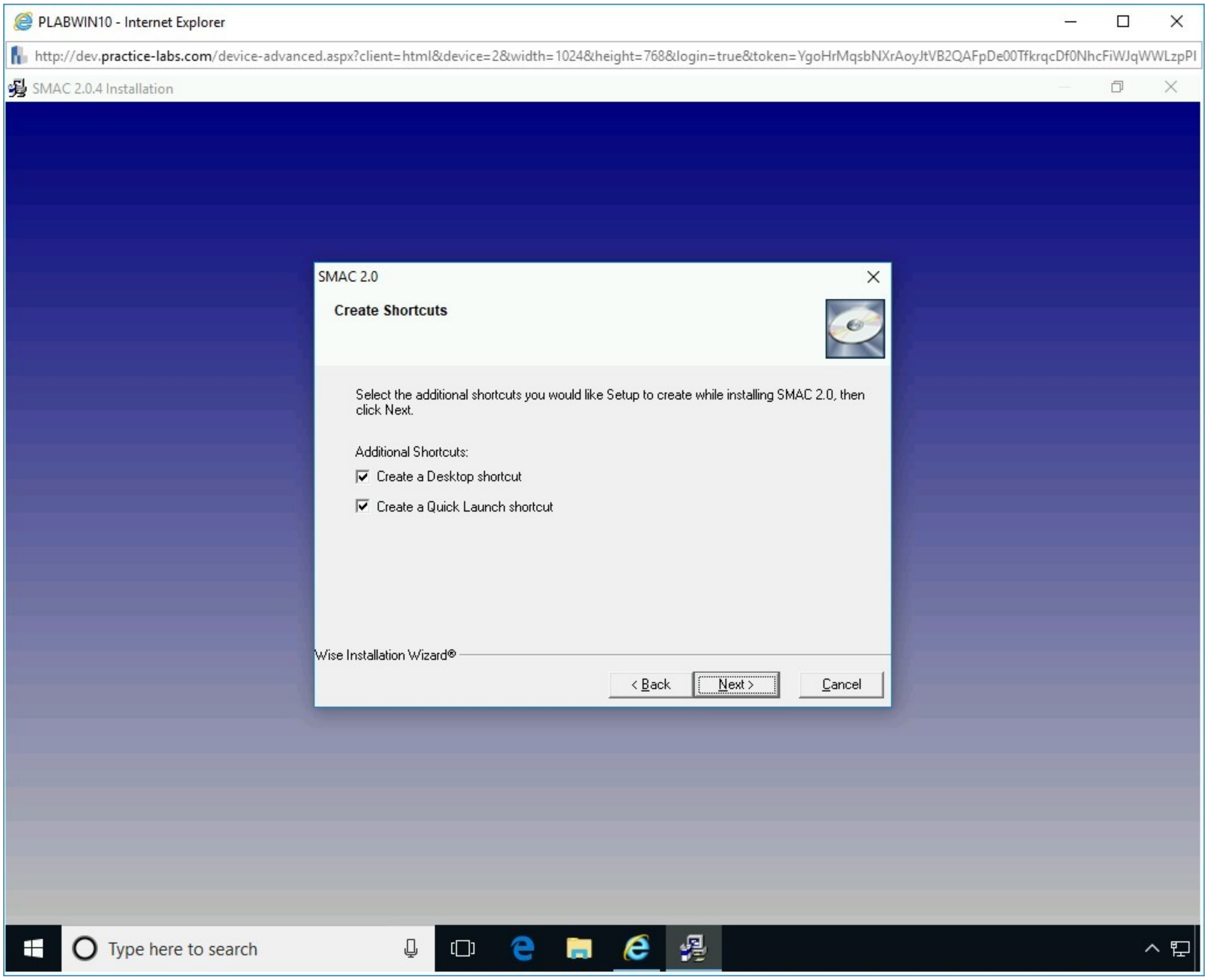
You can choose not to install SMAC 2.0 by clicking Cancel to exit Setup.

Destination Folder: C:\Program Files (x86)\KLC\SMAC

Figure 1.33 Screenshot of PLABWIN10: Clicking Next on the Destination Location page.

Step 6

On the **Create Shortcuts** page, keep the default selection and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
SMAC 2.0.4 Installation
SMAC 2.0
Wise Installation Wizard®
< Back
Next >
Cancel
Type here to search

Create Shortcuts

Select the additional shortcuts you would like Setup to create while installing SMAC 2.0, then click Next.

Additional Shortcuts:

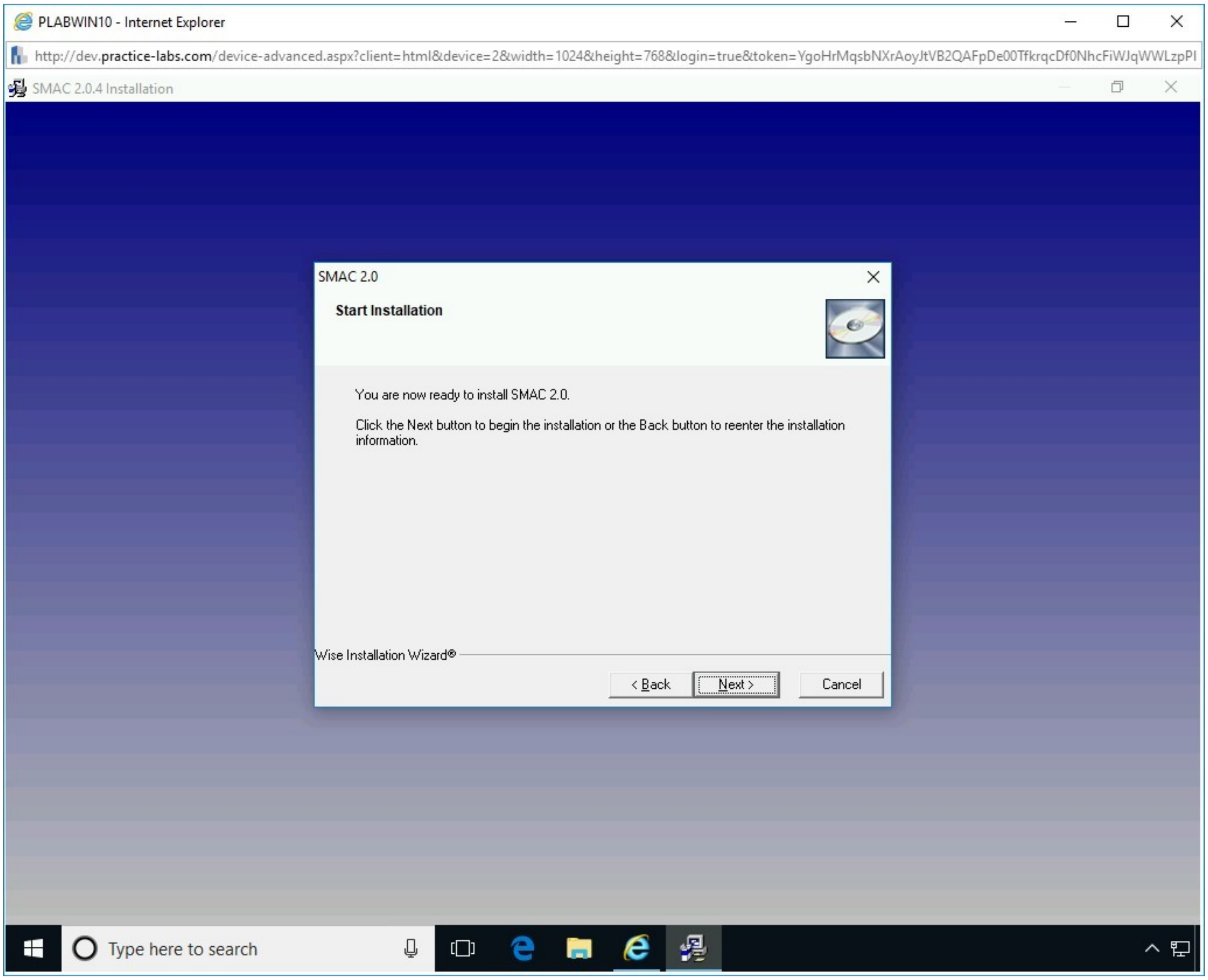
☑ Create a Desktop shortcut

☑ Create a Quick Launch shortcut

Figure 1.34 Screenshot of PLABWIN10: Keeping the default options and clicking Next on the Create Shortcuts page.

Step 7

On the **Start Installation** page, click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
SMAC 2.0.4 Installation
SMAC 2.0
Start Installation

You are now ready to install SMAC 2.0.

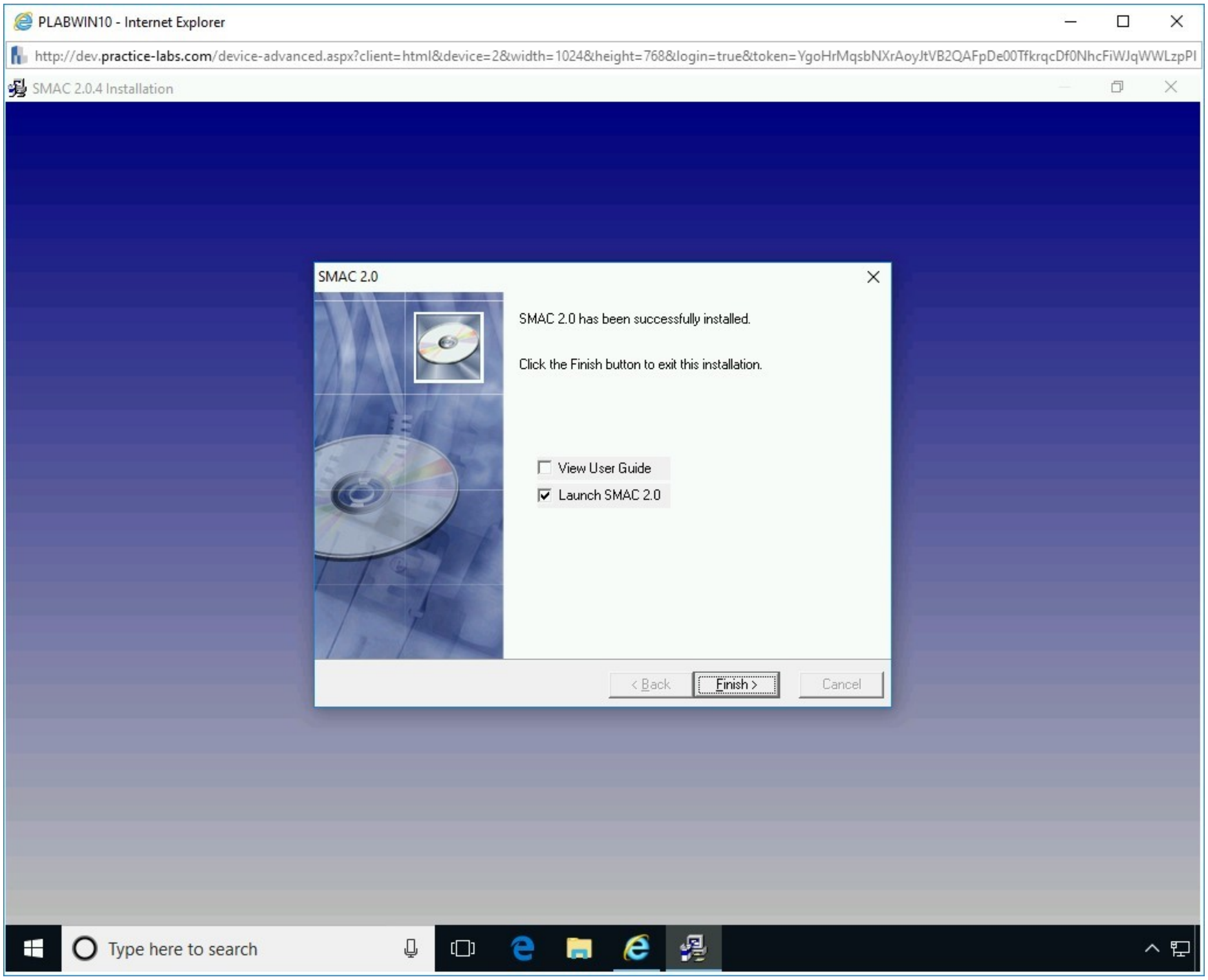
Click the Next button to begin the installation or the Back button to reenter the installation information.

Wise Installation Wizard®
< Back
Next >
Cancel
Type here to search

Figure 1.35 Screenshot of PLABWIN10: Clicking Next on the Start Installation page.

Step 8

The installation of SMAC will complete quickly. On the final page of the SMAC 2.0 wizard, keep the default selection, and click **Finish**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
SMAC 2.0.4 Installation
SMAC 2.0
< Back
Finish >
Cancel
Type here to search

SMAC 2.0 has been successfully installed.

Click the Finish button to exit this installation.

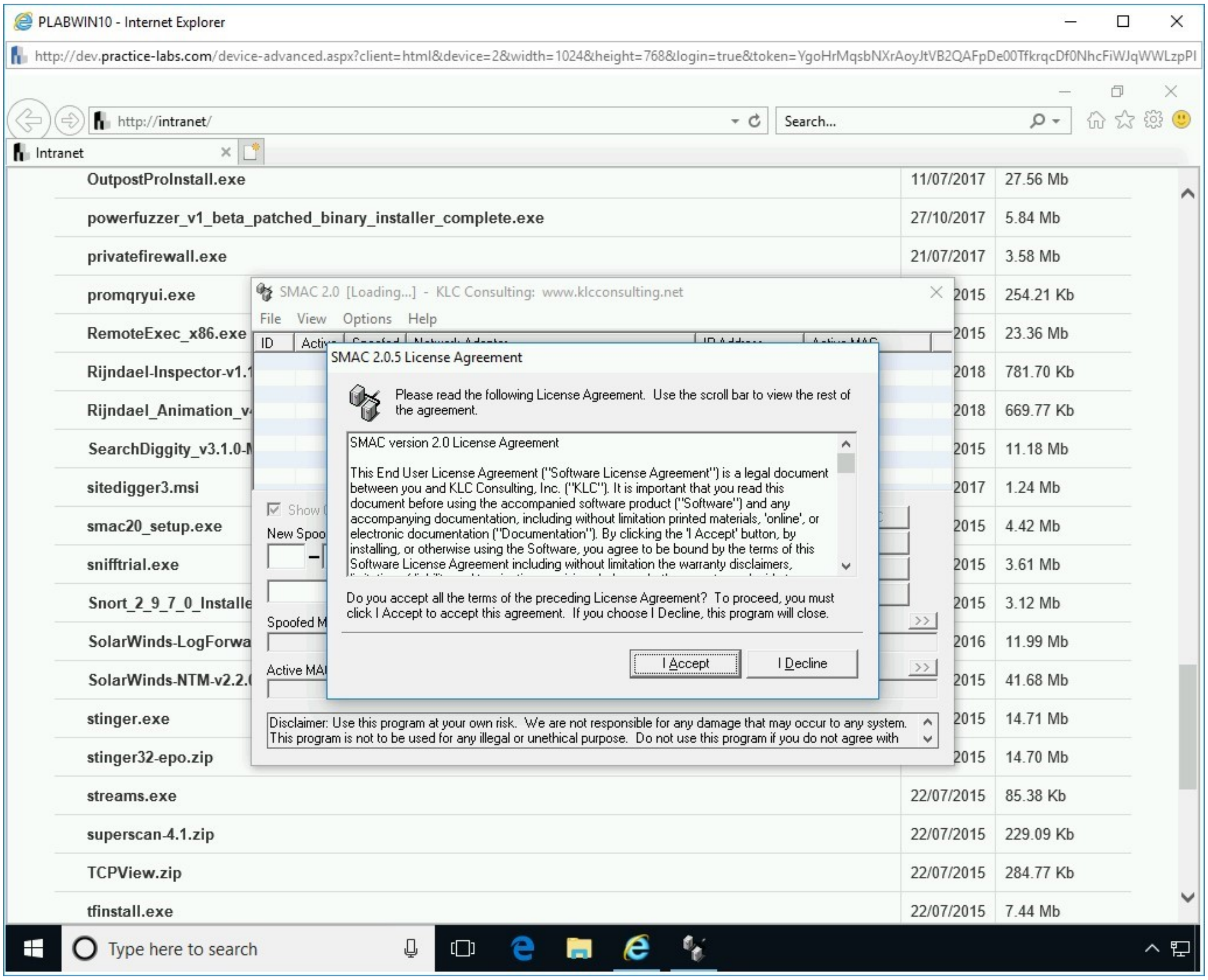
□ View User Guide

☑ Launch SMAC 2.0

Figure 1.36 Screenshot of PLABWIN10: Keeping the default option and clicking Finish.

Step 9

The **SMAC 2.0.5 License Agreement** is displayed. Click **I Accept**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
File View Options Help
ID Active Spoofed Network Adapter IP Address Active MAC
Show
New Spoo
Spoofed M
Active MA
Type here to search

OutpostProInstall.exe	11/07/2017	27.56 Mb
powerfuzzer_v1_beta_patched_binary_installer_complete.exe	27/10/2017	5.84 Mb
privatefirewall.exe	21/07/2017	3.58 Mb
promqryui.exe	2015	254.21 Kb
RemoteExec_x86.exe	2015	23.36 Mb
Rijndael-Inspector-v1.1	2018	781.70 Kb
Rijndael_Animation_v4	2018	669.77 Kb
SearchDiggity_v3.1.0-M	2015	11.18 Mb
sitedigger3.msi	2017	1.24 Mb
smac20_setup.exe	2015	4.42 Mb
snifftrial.exe	2015	3.61 Mb
Snort_2_9_7_0_Installe	2015	3.12 Mb
SolarWinds-LogForwa	2016	11.99 Mb
SolarWinds-NTM-v2.2.0	2015	41.68 Mb
stinger.exe	2015	14.71 Mb
stinger32-epo.zip	2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb

SMAC 2.0 [Loading...] - KLC Consulting: www.klcconsulting.net

SMAC 2.0.5 License Agreement

Please read the following License Agreement. Use the scroll bar to view the rest of the agreement.

SMAC version 2.0 License Agreement

This End User License Agreement ("Software License Agreement") is a legal document between you and KLC Consulting, Inc. ("KLC"). It is important that you read this document before using the accompanied software product ("Software") and any accompanying documentation, including without limitation printed materials, 'online', or electronic documentation ("Documentation"). By clicking the 'I Accept' button, by installing, or otherwise using the Software, you agree to be bound by the terms of this Software License Agreement including without limitation the warranty disclaimers,

Do you accept all the terms of the preceding License Agreement? To proceed, you must click I Accept to accept this agreement. If you choose I Decline, this program will close.

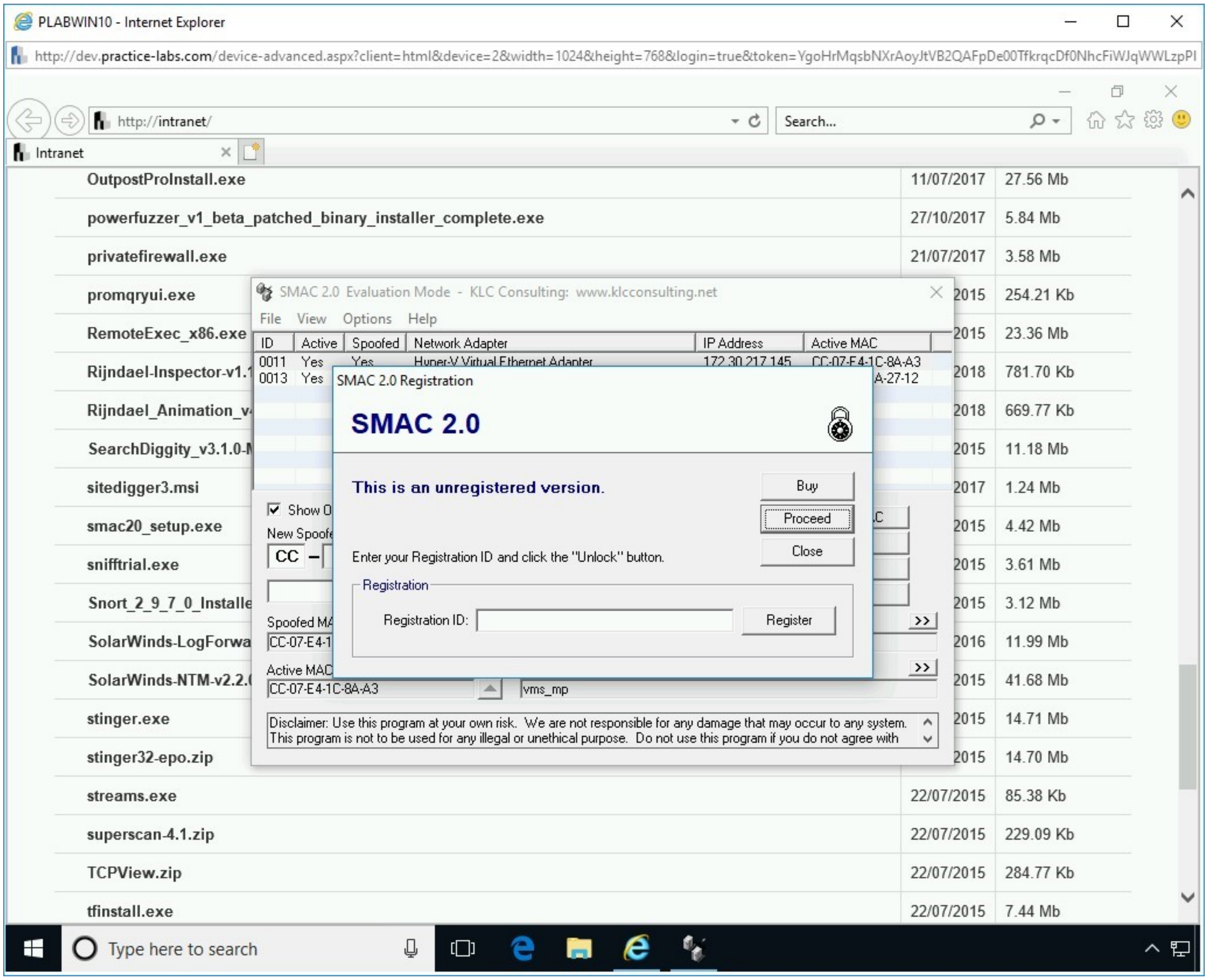
I Accept | I Decline

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.37 Screenshot of PLABWIN10: Clicking I Accept on the SMAC 2.0.5 License Agreement dialog box.

Step 10

The **SMAC 2.0 Registration** dialog box is displayed. Click **Proceed**.



SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes				A-27-12

SMAC 2.0 Registration

SMAC 2.0

This is an unregistered version.

Enter your Registration ID and click the "Unlock" button.

Registration ID:

Active MAC: CC-07-E4-1C-8A-A3 vms_mp

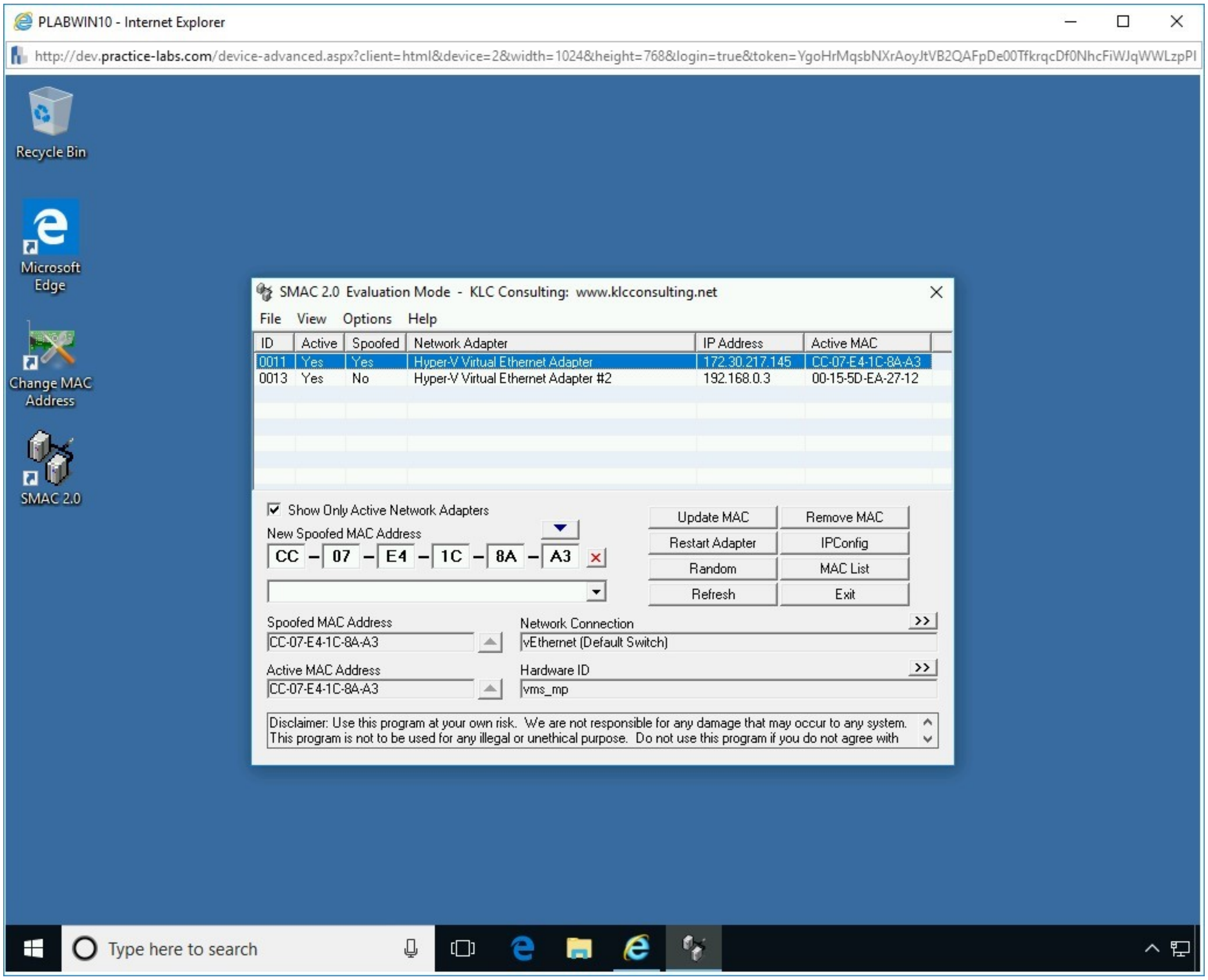
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.38 Screenshot of PLABWIN10: Clicking Proceed on the SMAC 2.0 Registration page.

Step 11

Minimize Internet Explorer from the background of SMAC 2.0. The **SMAC 2.0 Evaluation Mode** dialog box is displayed. Note that it displays the MAC addresses of two NICs that exist in the system.

> ***Note:*** *If you have performed the previous task, you will remember that you had changed the MAC address and manufacturer. The same MAC address still exists in the system.*



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI

SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes	No	Hyper-V Virtual Ethernet Adapter #2	192.168.0.3	00-15-5D-EA-27-12

☑ Show Only Active Network Adapters

New Spoofed MAC Address: CC – 07 – E4 – 1C – 8A – A3

Spoofed MAC Address: CC-07-E4-1C-8A-A3

Active MAC Address: CC-07-E4-1C-8A-A3

Network Connection: vEthernet (Default Switch)

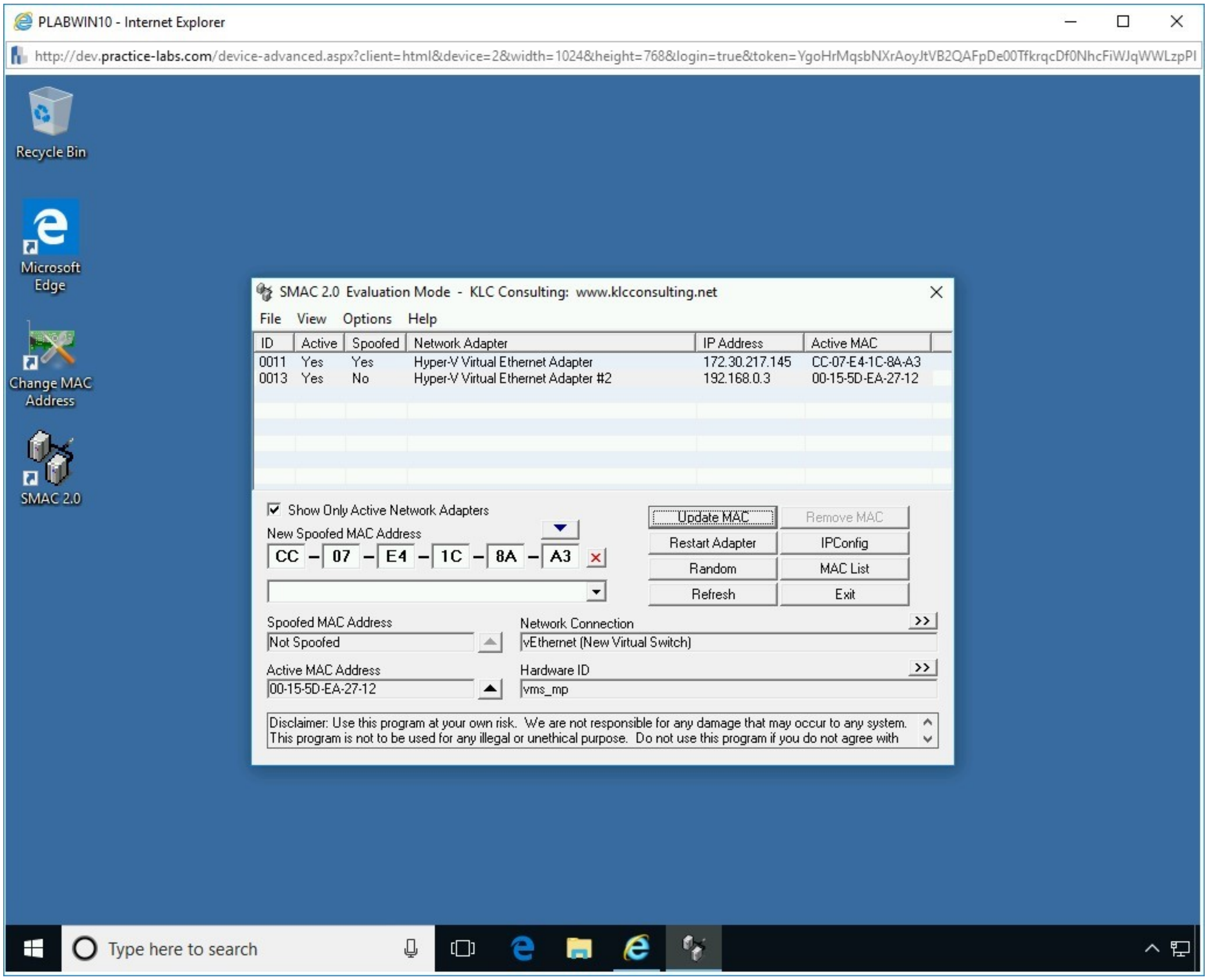
Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.39 Screenshot of PLABWIN10: Showing the SMAC 2.0 Evaluation Mode dialog box.

Step 12

From the top section, select the **NIC** with **ID 0013** and click **Update MAC**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Recycle Bin
Microsoft Edge
Change MAC Address
SMAC 2.0
SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File
View
Options
Help
Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit
Type here to search

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes	No	Hyper-V Virtual Ethernet Adapter #2	192.168.0.3	00-15-5D-EA-27-12

☑ Show Only Active Network Adapters

New Spoofed MAC Address: CC – 07 – E4 – 1C – 8A – A3

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (New Virtual Switch)

Active MAC Address: 00-15-5D-EA-27-12

Hardware ID: vms_mp

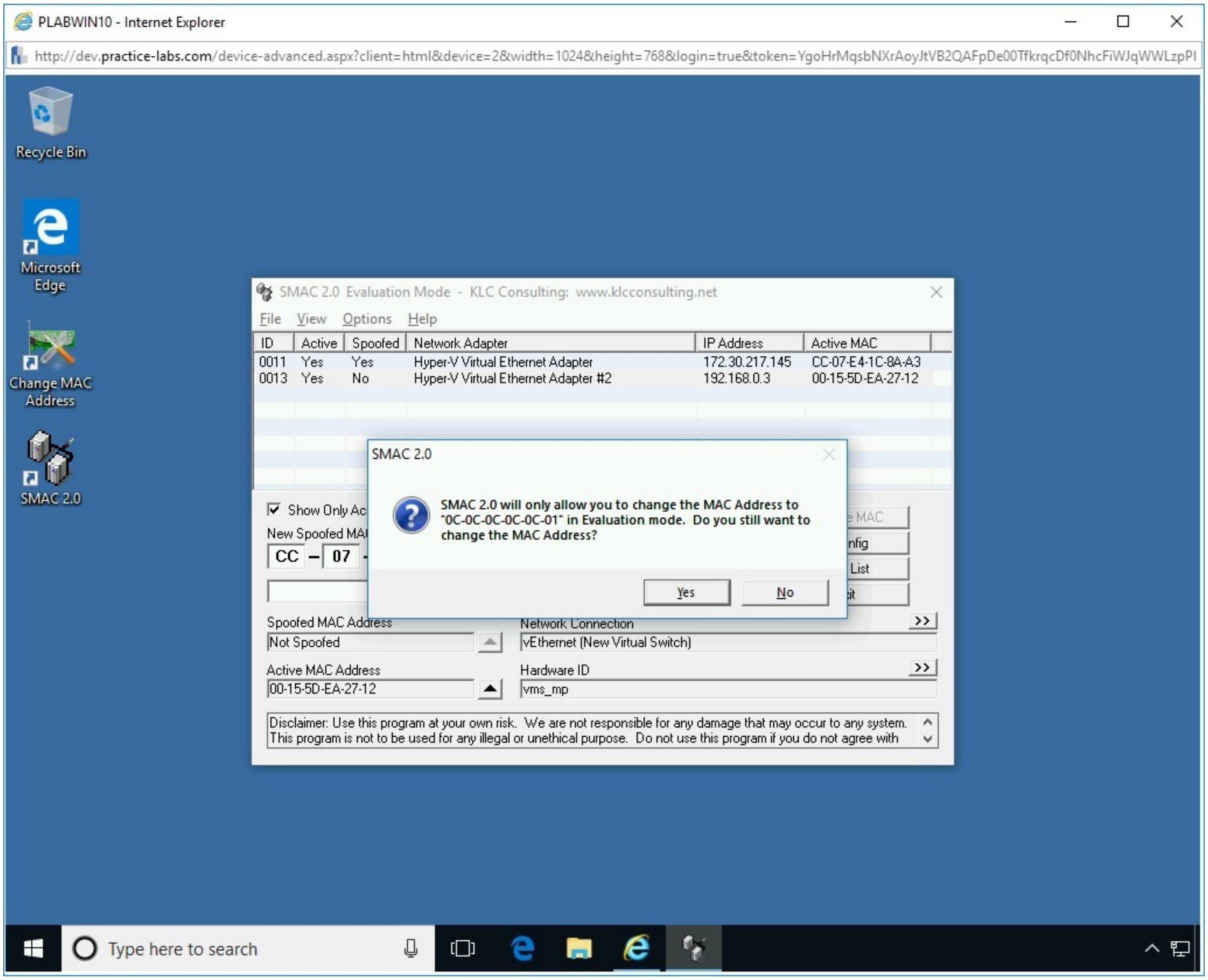
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.40 Screenshot of PLABWIN10: Selecting a NIC and clicking Update MAC on the SMAC 2.0 Evaluation Mode dialog box.

Step 13

The **SMAC 2.0** dialog box is displayed. Since you are using an evaluation version, there is only a fixed MAC address to which the current MAC address will change.

Click **Yes**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
Recycle Bin
Microsoft Edge
Change MAC Address
SMAC 2.0
SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File
View
Options
Help
☑ Show Only Ac
New Spoofed MAC
CC
07
MAC
nfig
List
it
>>
Type here to search

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes	No	Hyper-V Virtual Ethernet Adapter #2	192.168.0.3	00-15-5D-EA-27-12

SMAC 2.0

SMAC 2.0 will only allow you to change the MAC Address to "0C-0C-0C-0C-0C-01" in Evaluation mode. Do you still want to change the MAC Address?

Yes No

Spoofed MAC Address: Not Spoofed

Network Connection: vEthernet (New Virtual Switch)

Active MAC Address: 00-15-5D-EA-27-12

Hardware ID: vms_mp

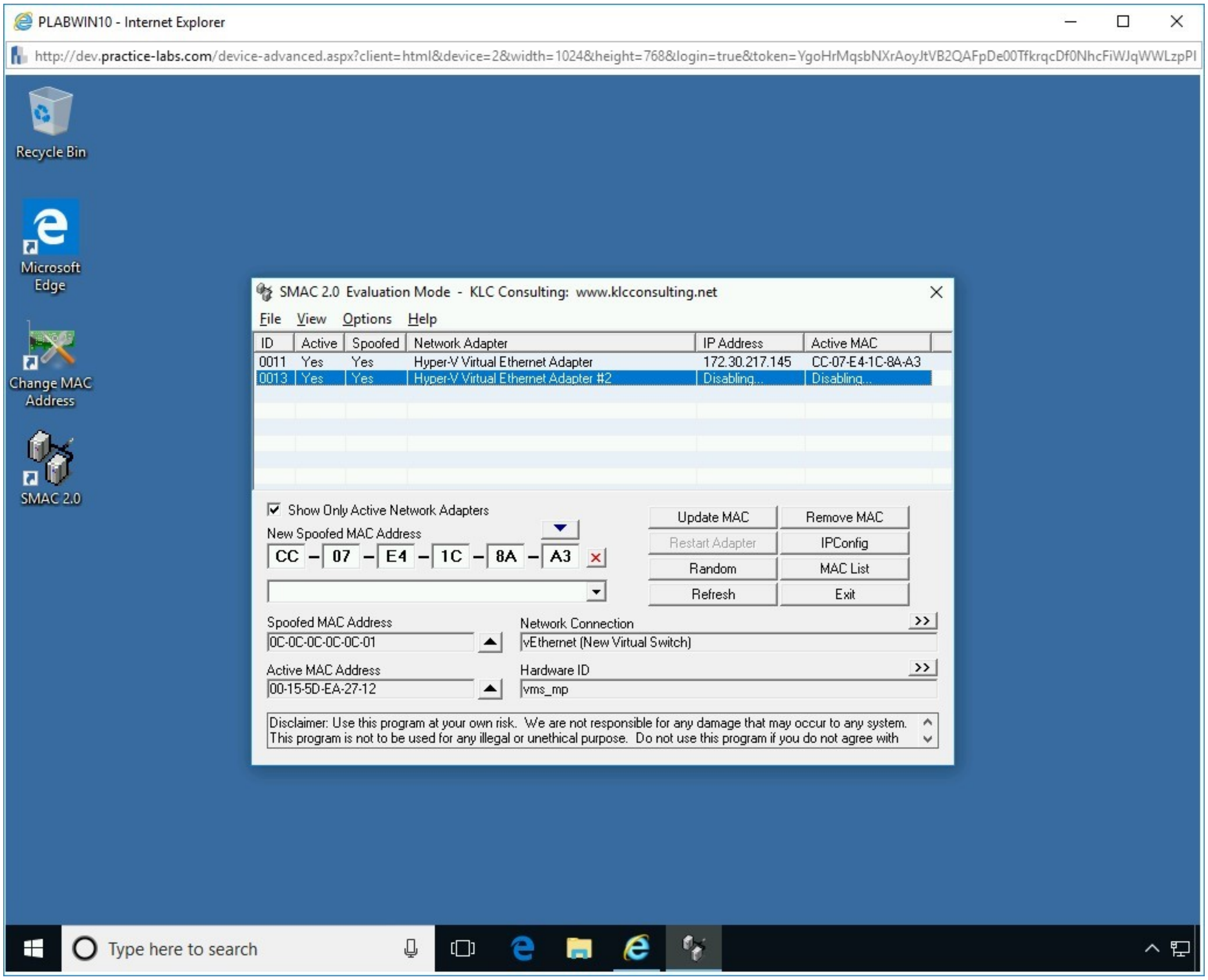
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.41 Screenshot of PLABWIN10: Clicking Yes on the SMAC 2.0 dialog box.

Step 14

The MAC address change process starts.

Note: *Disabling is mentioned under the IP Address and Active MAC columns.*


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Recycle Bin
Microsoft Edge
Change MAC Address
SMAC 2.0
SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File
View
Options
Help
Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit
Type here to search

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes	Yes	Hyper-V Virtual Ethernet Adapter #2	Disabling...	Disabling...

☑ Show Only Active Network Adapters

New Spoofed MAC Address: CC – 07 – E4 – 1C – 8A – A3

Spoofed MAC Address: 0C-0C-0C-0C-0C-01

Network Connection: vEthernet (New Virtual Switch)

Active MAC Address: 00-15-5D-EA-27-12

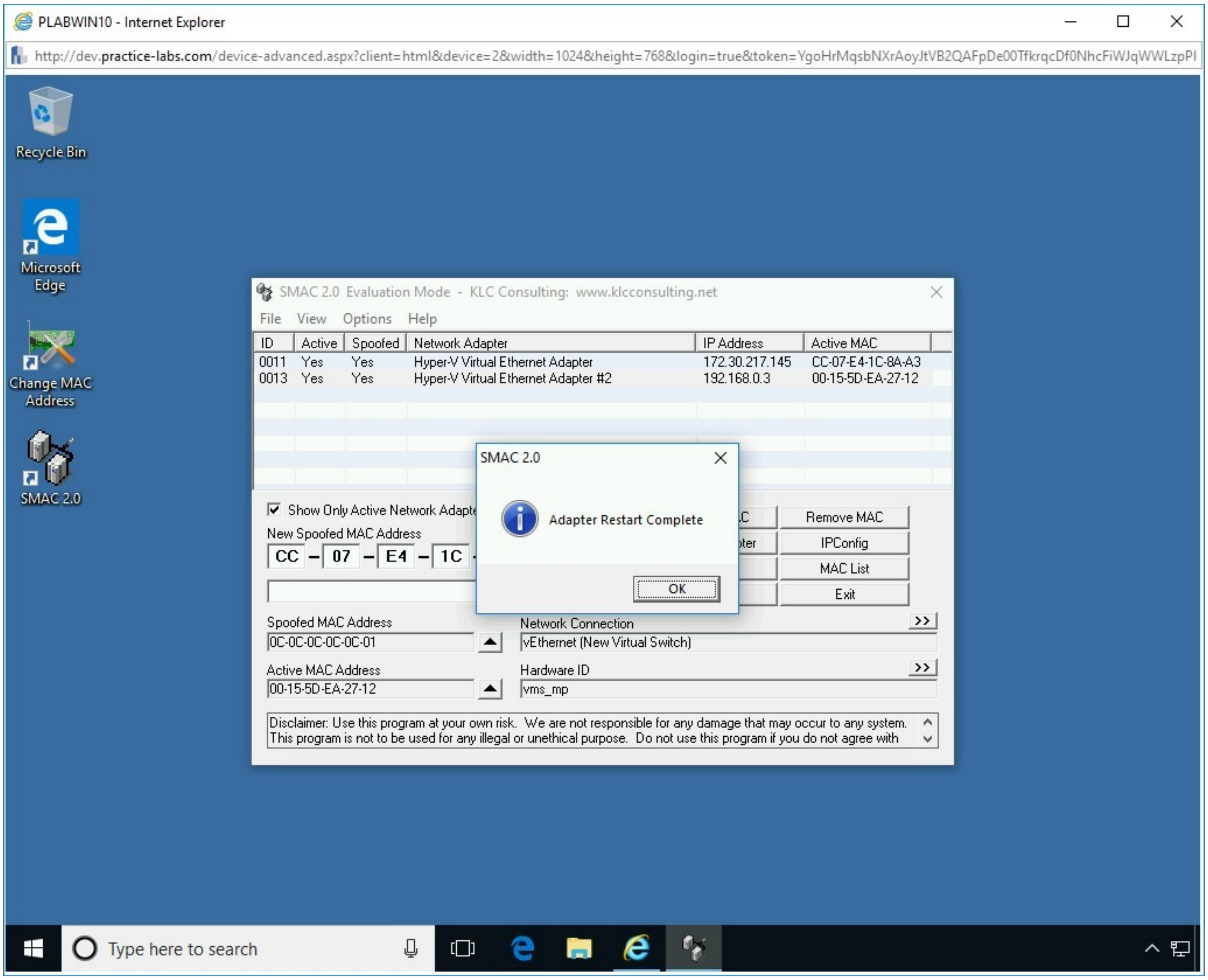
Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.42 Screenshot of PLABWIN10: Showing the MAC change process on the SMAC 2.0 Evaluation Mode dialog box.

Step 15

The **SMAC 2.0** dialog box is displayed. Click **OK**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI

SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes	Yes	Hyper-V Virtual Ethernet Adapter #2	192.168.0.3	00-15-5D-EA-27-12

☑ Show Only Active Network Adapte

New Spoofed MAC Address: CC – 07 – E4 – 1C –

SMAC 2.0

Adapter Restart Complete

OK

Spoofed MAC Address: 0C-0C-0C-0C-0C-01

Network Connection: vEthernet (New Virtual Switch)

Active MAC Address: 00-15-5D-EA-27-12

Hardware ID: vms_mp

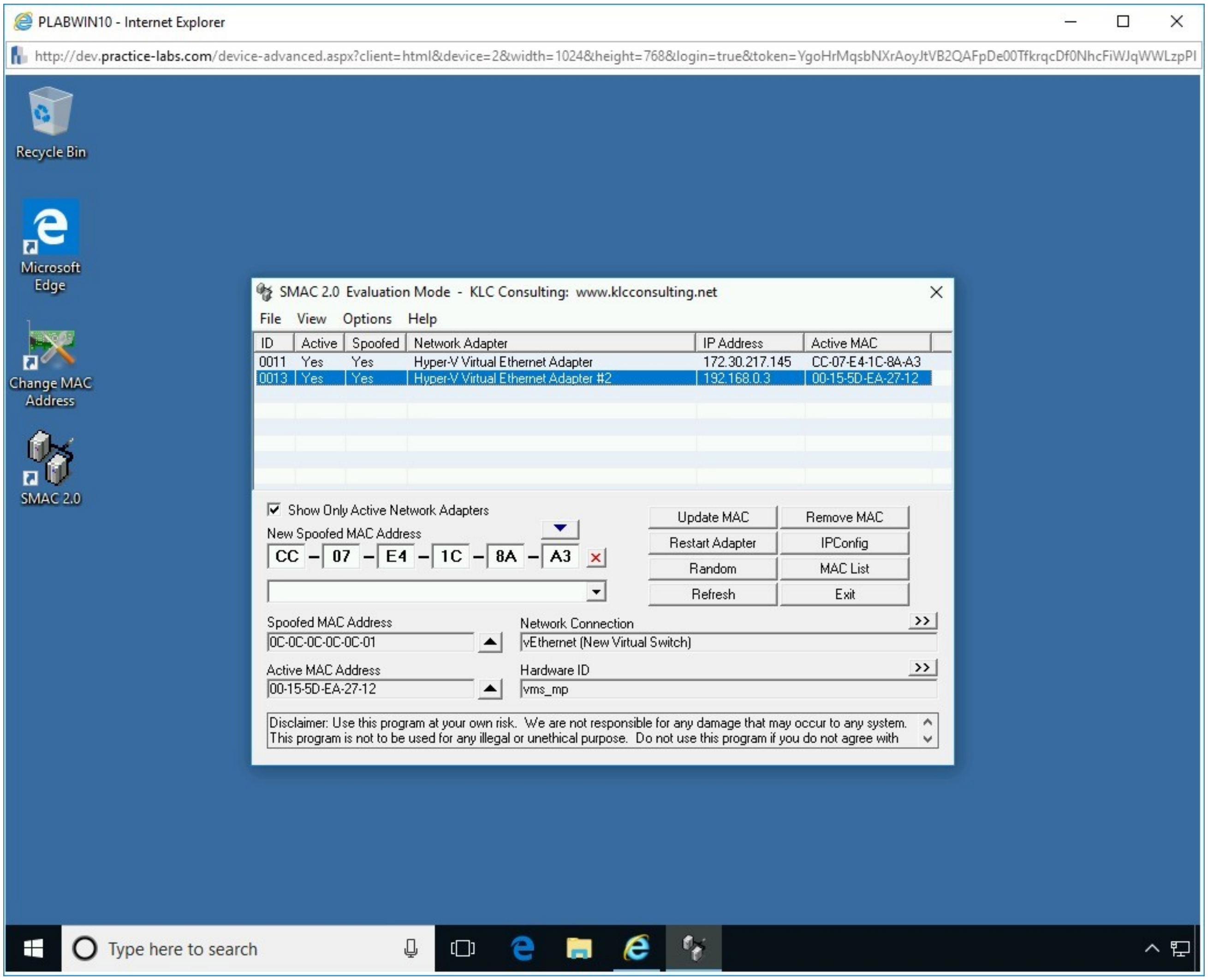
Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.43 Screenshot of PLABWIN10: Clicking OK on the SMAC 2.0 dialog box.

Step 16

The **Spoofed MAC Address** field now displays the spoofed MAC address.

Close the **SMAC 2.0** window.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
Recycle Bin
Microsoft Edge
Change MAC Address
SMAC 2.0
SMAC 2.0 Evaluation Mode - KLC Consulting: www.klcconsulting.net
File
View
Options
Help
Update MAC
Remove MAC
Restart Adapter
IPConfig
Random
MAC List
Refresh
Exit
Type here to search

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0011	Yes	Yes	Hyper-V Virtual Ethernet Adapter	172.30.217.145	CC-07-E4-1C-8A-A3
0013	Yes	Yes	Hyper-V Virtual Ethernet Adapter #2	192.168.0.3	00-15-5D-EA-27-12

☑ Show Only Active Network Adapters

New Spoofed MAC Address: CC – 07 – E4 – 1C – 8A – A3

Spoofed MAC Address: 0C-0C-0C-0C-0C-01

Network Connection: vEthernet (New Virtual Switch)

Active MAC Address: 00-15-5D-EA-27-12

Hardware ID: vms_mp

Disclaimer: Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with

Figure 1.44 Screenshot of PLABWIN10: Showing the spoofed MAC address on the SMAC 2.0 Evaluation Mode dialog box.

Task 3 - Install Wireshark

Wireshark is a packet capturing tool. It can capture packets that traverse through the network. You can use Wireshark for also sniffing the network traffic.

In this task, you will learn to install Wireshark. To do this, perform the following steps:

Step 1

Ensure you have powered on the required devices and connected to **PLABWIN10**.

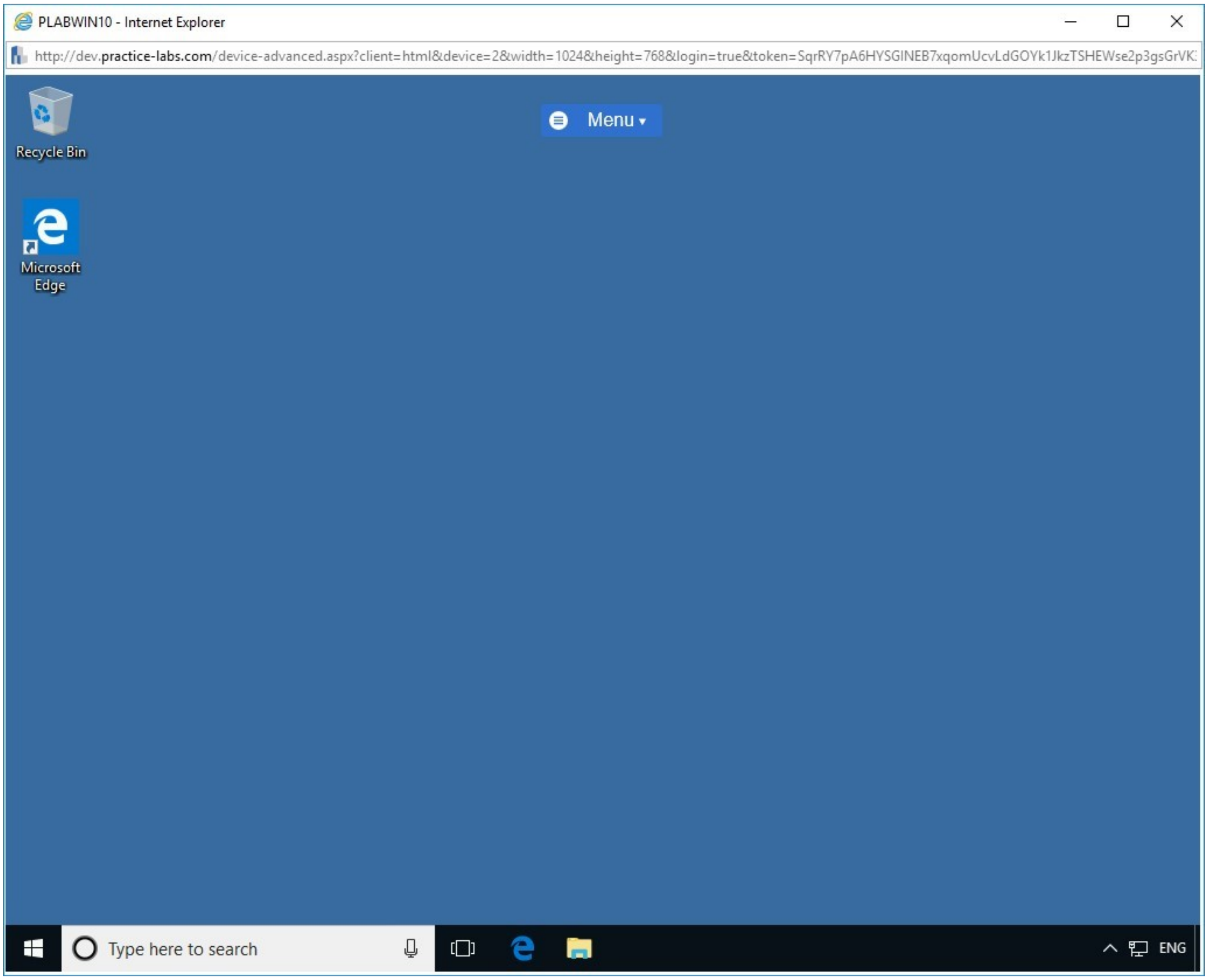

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
Menu
Recycle Bin
Microsoft Edge
Type here to search
ENG

Figure 1.45 Screenshot of PLABWIN10: Showing the desktop of PLABWIN10.

Step 2

In the **Type here to search** text box, type the following:

```
Internet Explorer
```

From the search results, select **Internet Explorer**.

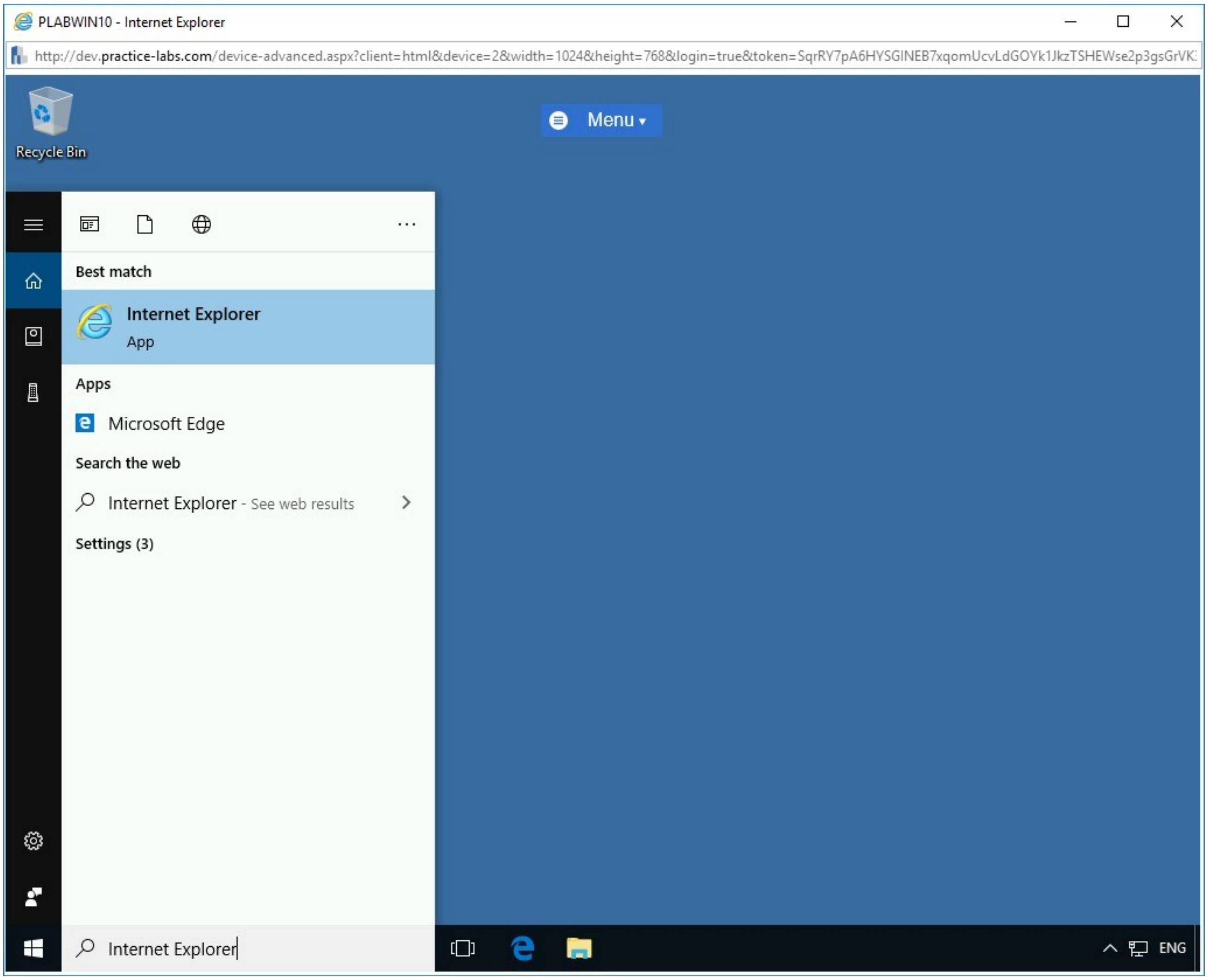
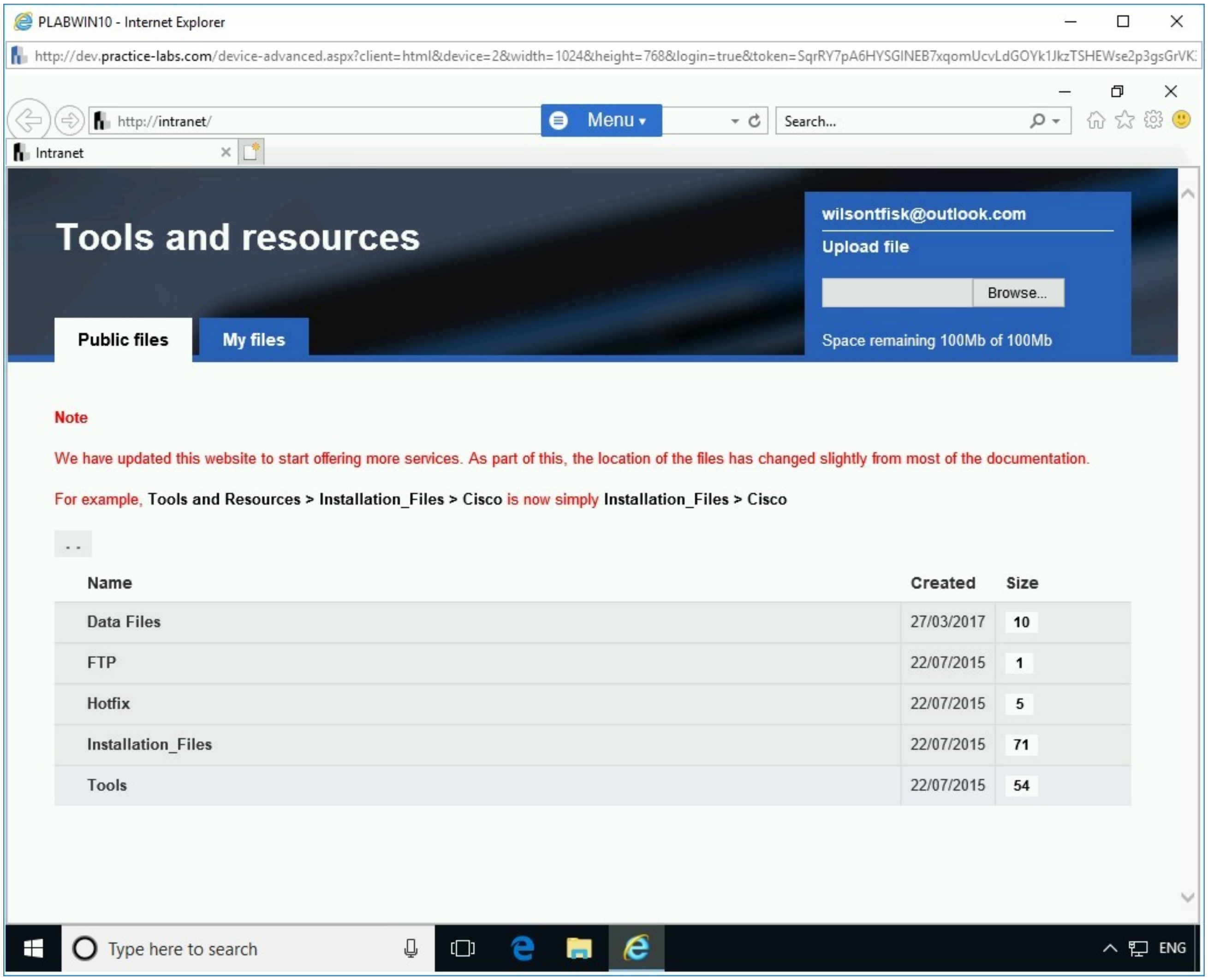

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
Recycle Bin
Menu
Best match
Internet Explorer
App
Apps
Microsoft Edge
Search the web
Internet Explorer - See web results
Settings (3)
Internet Explorer
ENG

Figure 1.46 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 3

The **Intranet** Website is displayed. On the **Intranet** homepage, click **Tools**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
http://intranet/
Menu
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search
ENG

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, Tools and Resources > Installation_Files > Cisco is now simply Installation_Files > Cisco

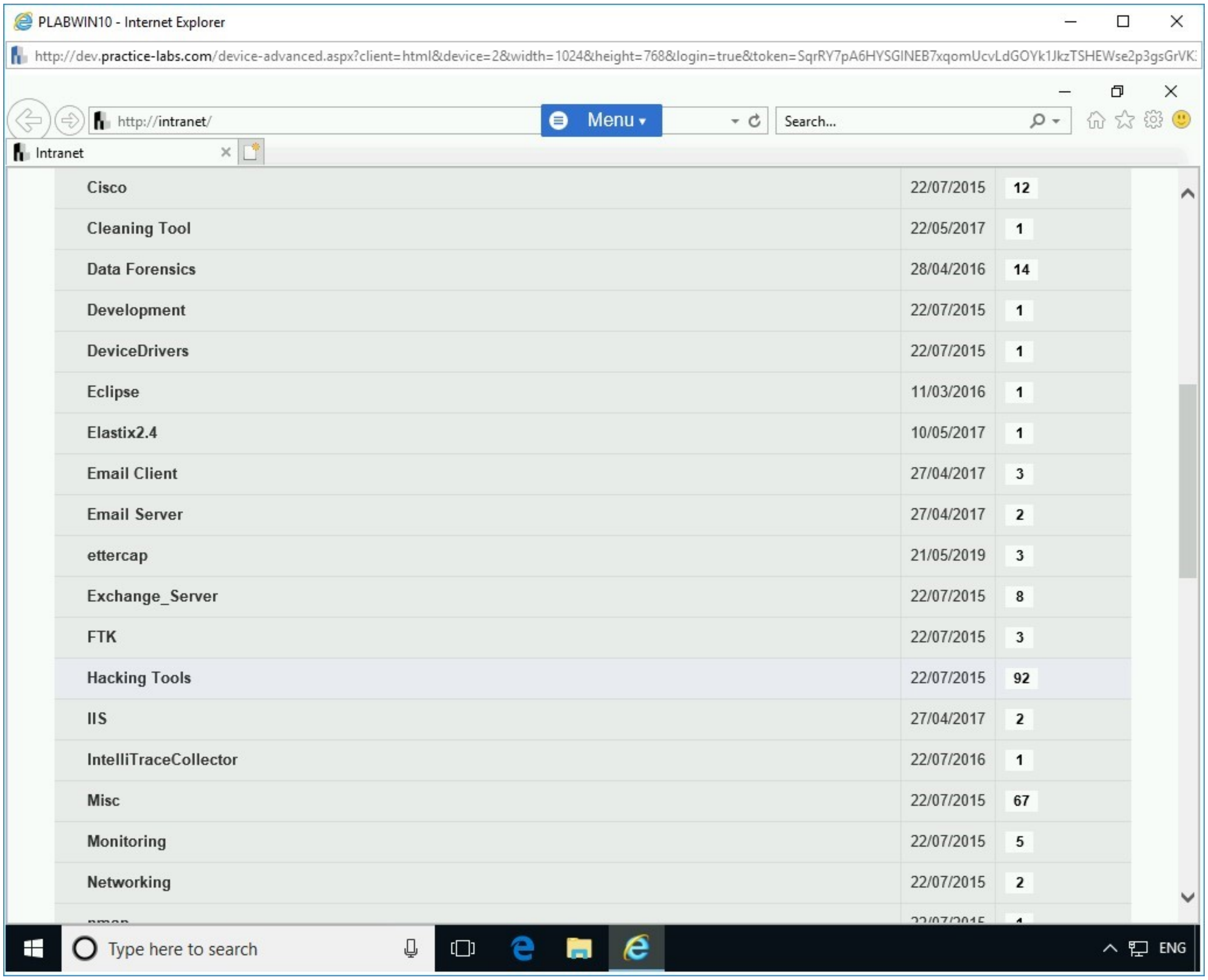
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	71
Tools	22/07/2015	54

Figure 1.47 Screenshot of PLABWIN10: Internet Explorer Intranet page displayed. Clicking Tools on the Intranet homepage.

Step 4

On the **Tools** Webpage, click **Hacking Tools**.

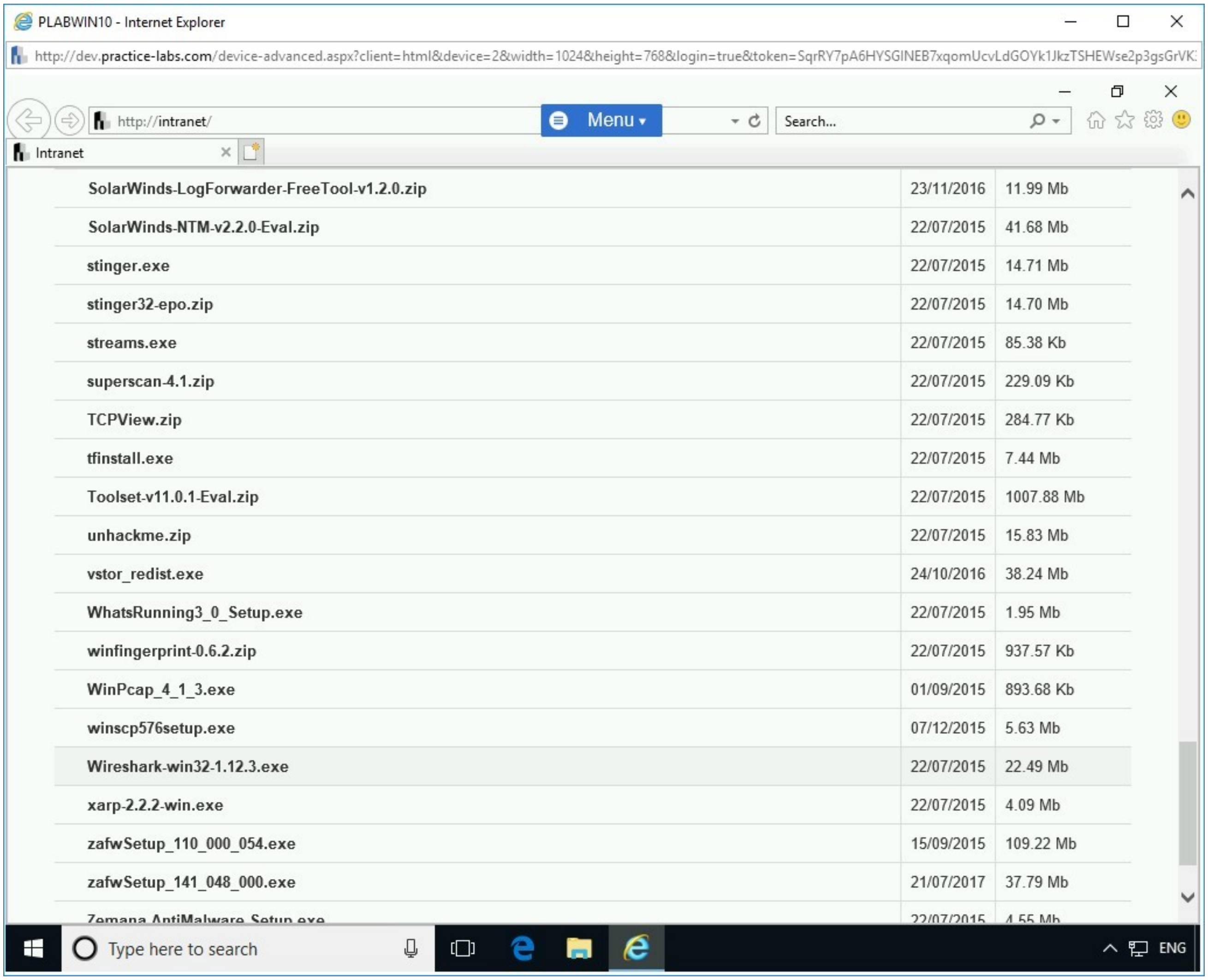

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
http://intranet/
Menu
Search...
Intranet
Type here to search
ENG

Cisco	22/07/2015	12
Cleaning Tool	22/05/2017	1
Data Forensics	28/04/2016	14
Development	22/07/2015	1
DeviceDrivers	22/07/2015	1
Eclipse	11/03/2016	1
Elastix2.4	10/05/2017	1
Email Client	27/04/2017	3
Email Server	27/04/2017	2
ettercap	21/05/2019	3
Exchange_Server	22/07/2015	8
FTK	22/07/2015	3
Hacking Tools	22/07/2015	92
IIS	27/04/2017	2
IntelliTraceCollector	22/07/2016	1
Misc	22/07/2015	67
Monitoring	22/07/2015	5
Networking	22/07/2015	2
nmap	22/07/2015	1

Figure 1.48 Screenshot of PLABWIN10: Clicking Hacking Tools on the Intranet homepage.

Step 5

Locate and click **Wireshark-win32-1.12.3.exe**.

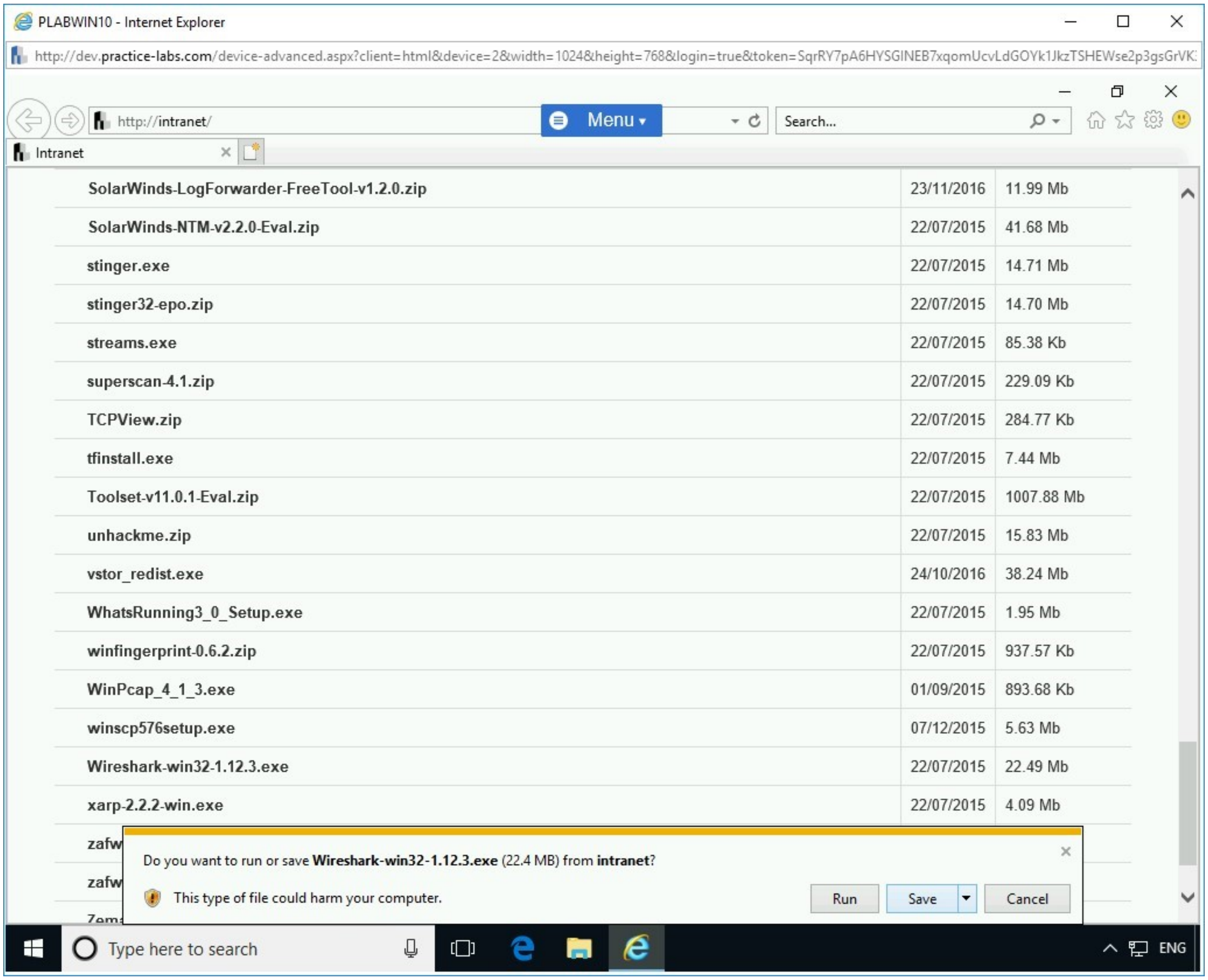

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK:
http://intranet/
Menu
Search...
Intranet
Type here to search
ENG

SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana AntiMalware Setup.exe	22/07/2015	4.55 Mb

Figure 1.49 Screenshot of PLABWIN10: Clicking Wireshark-win32-1.12.3.exe on the Intranet homepage.

Step 6

In the notification bar, click **Save**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
http://intranet/
Menu
Search...
Intranet
Run
Save
Cancel
Type here to search
ENG

SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafw		
zafw		

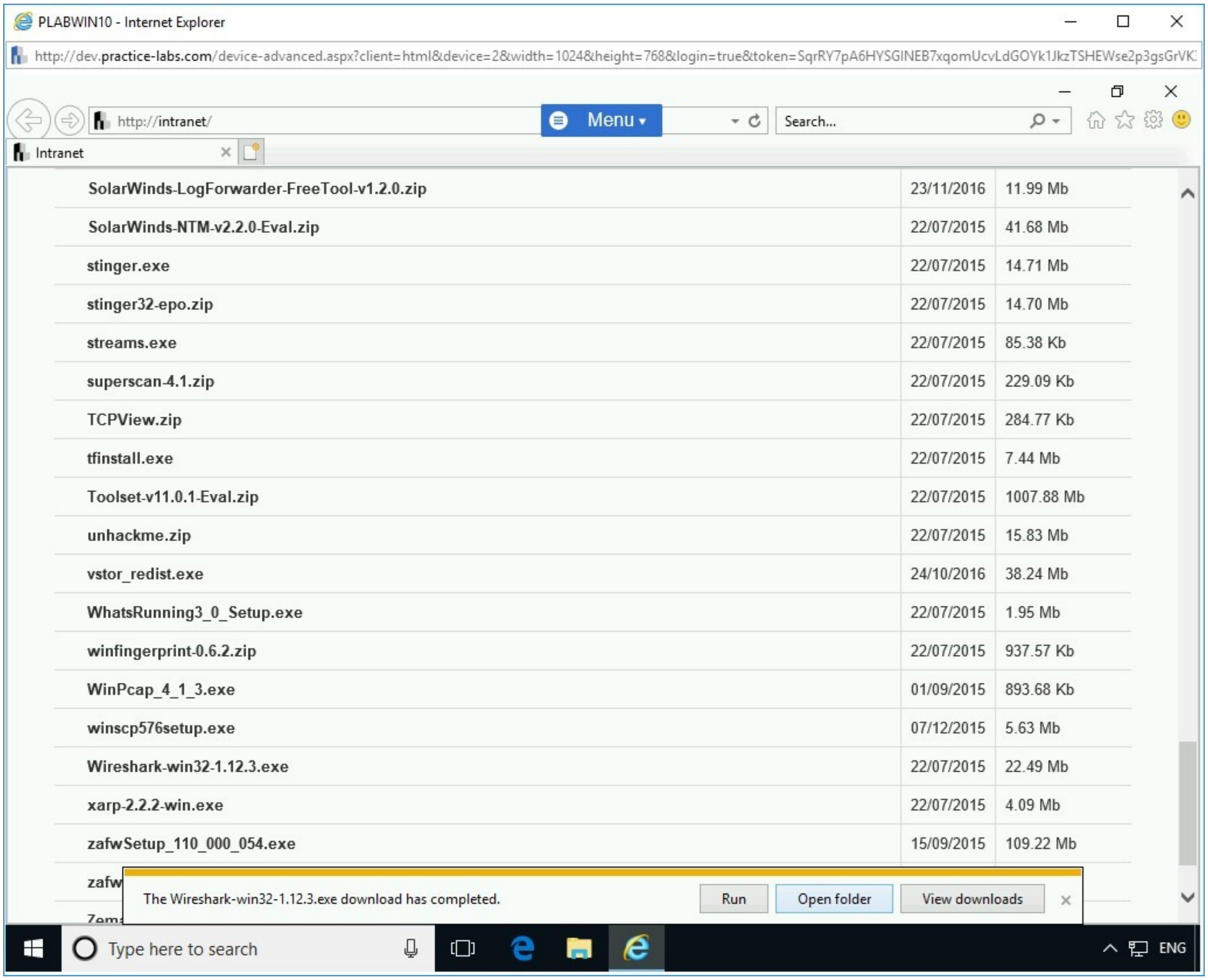
Do you want to run or save **Wireshark-win32-1.12.3.exe** (22.4 MB) from **intranet**?

This type of file could harm your computer.

Figure 1.50 Screenshot of PLABWIN10: Clicking the Save option in the notification bar.

Step 7

In the notification bar, click **Open folder**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
http://intranet/
Menu
Search...
Intranet
Run
Open folder
View downloads
Type here to search
ENG

SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb

The Wireshark-win32-1.12.3.exe download has completed.

Figure 1.51 Screenshot of PLABWIN10: Clicking the Open folder option in the notification bar.

Step 8

The **File Explorer** downloads window is now open. Double-click the **Wireshark-win32-1.12.3.exe** file.

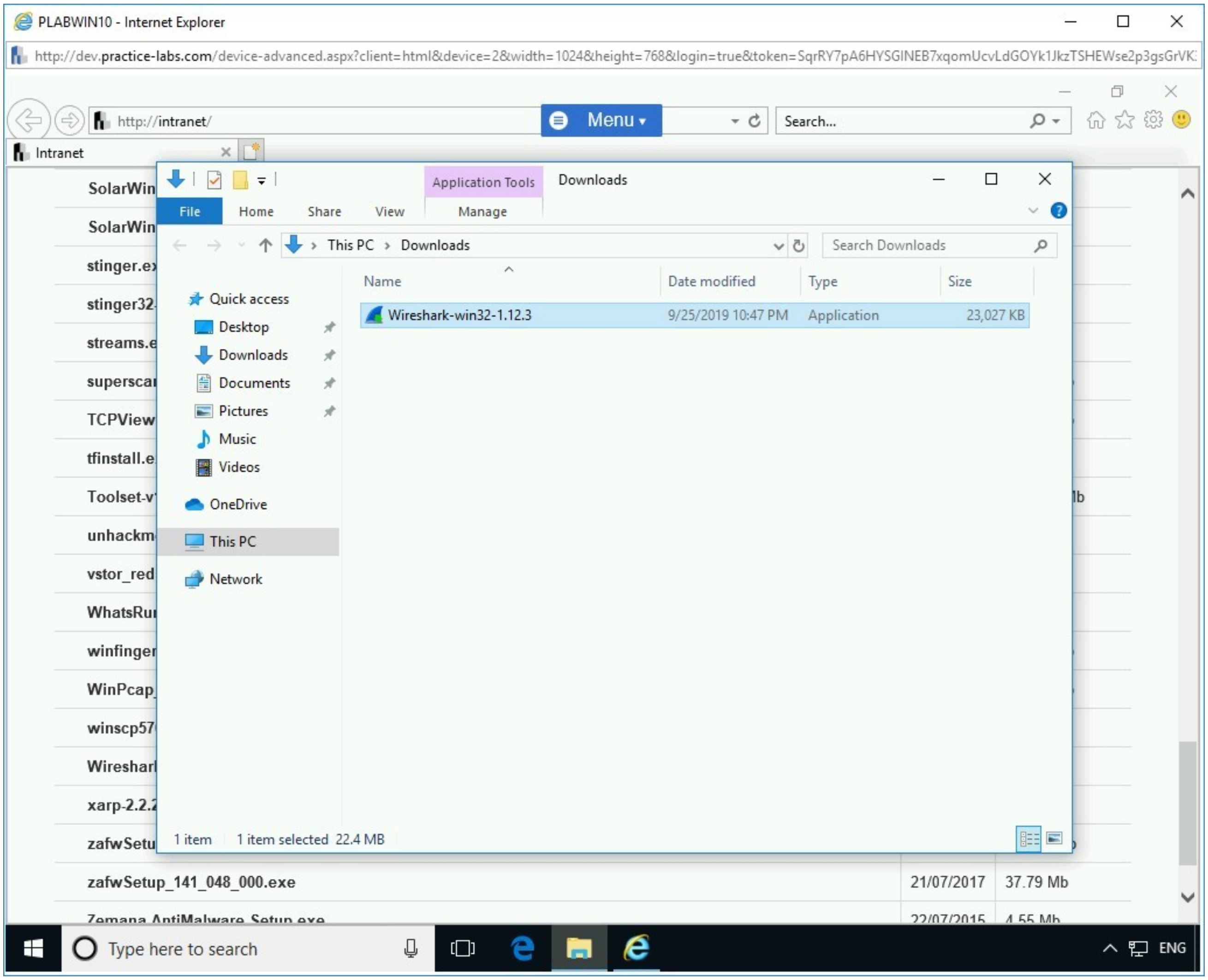
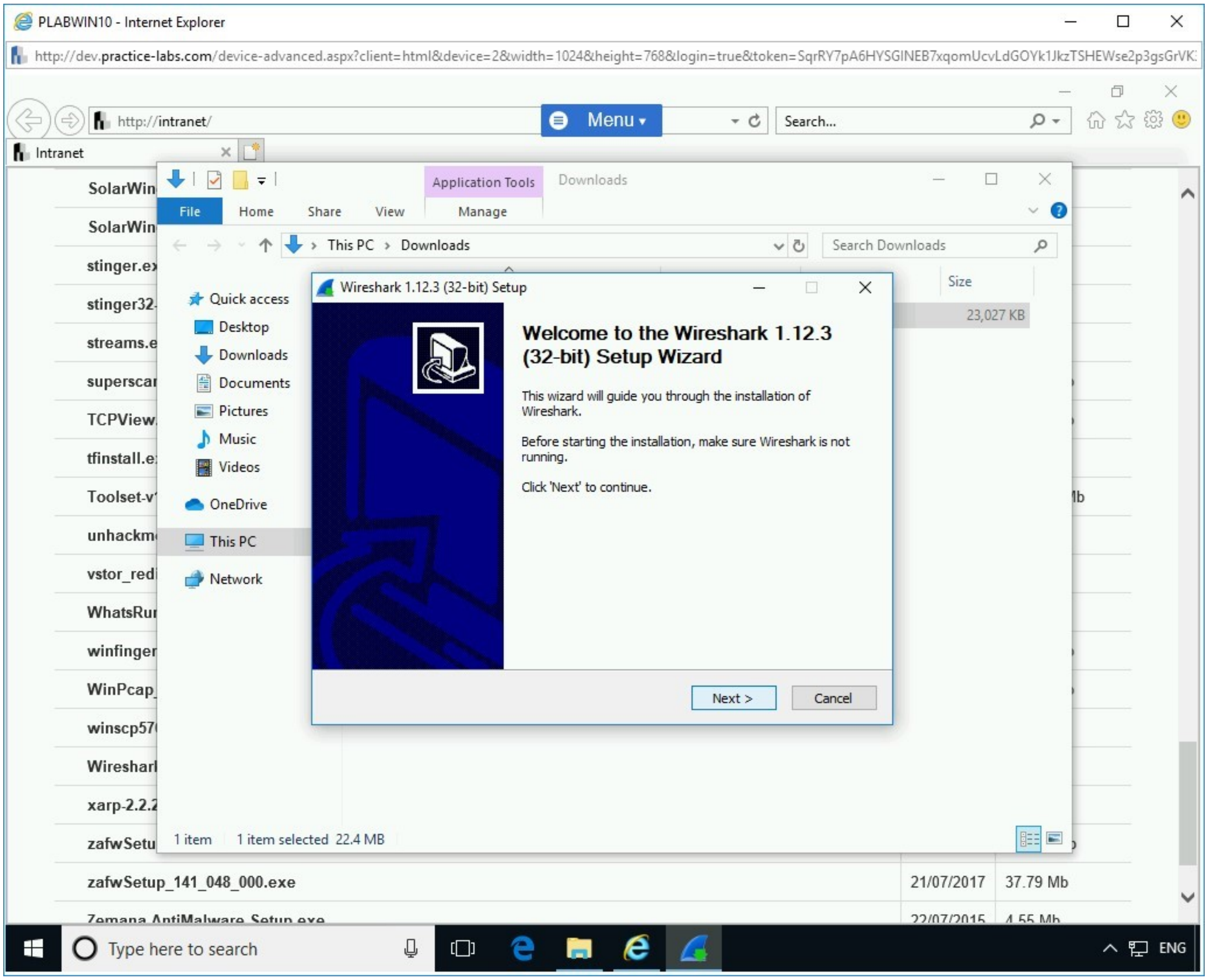


Figure 1.52 Screenshot of PLABWIN10: Double-clicking the Wireshark-win32-1.12.3.exe file in the File Explorer Downloads window.

Step 9

The **Welcome to the Wireshark 1.12.3 (32-bit) Setup Wizard** is displayed. Click **Next** to continue.



Welcome to the Wireshark 1.12.3 (32-bit) Setup Wizard

This wizard will guide you through the installation of Wireshark.

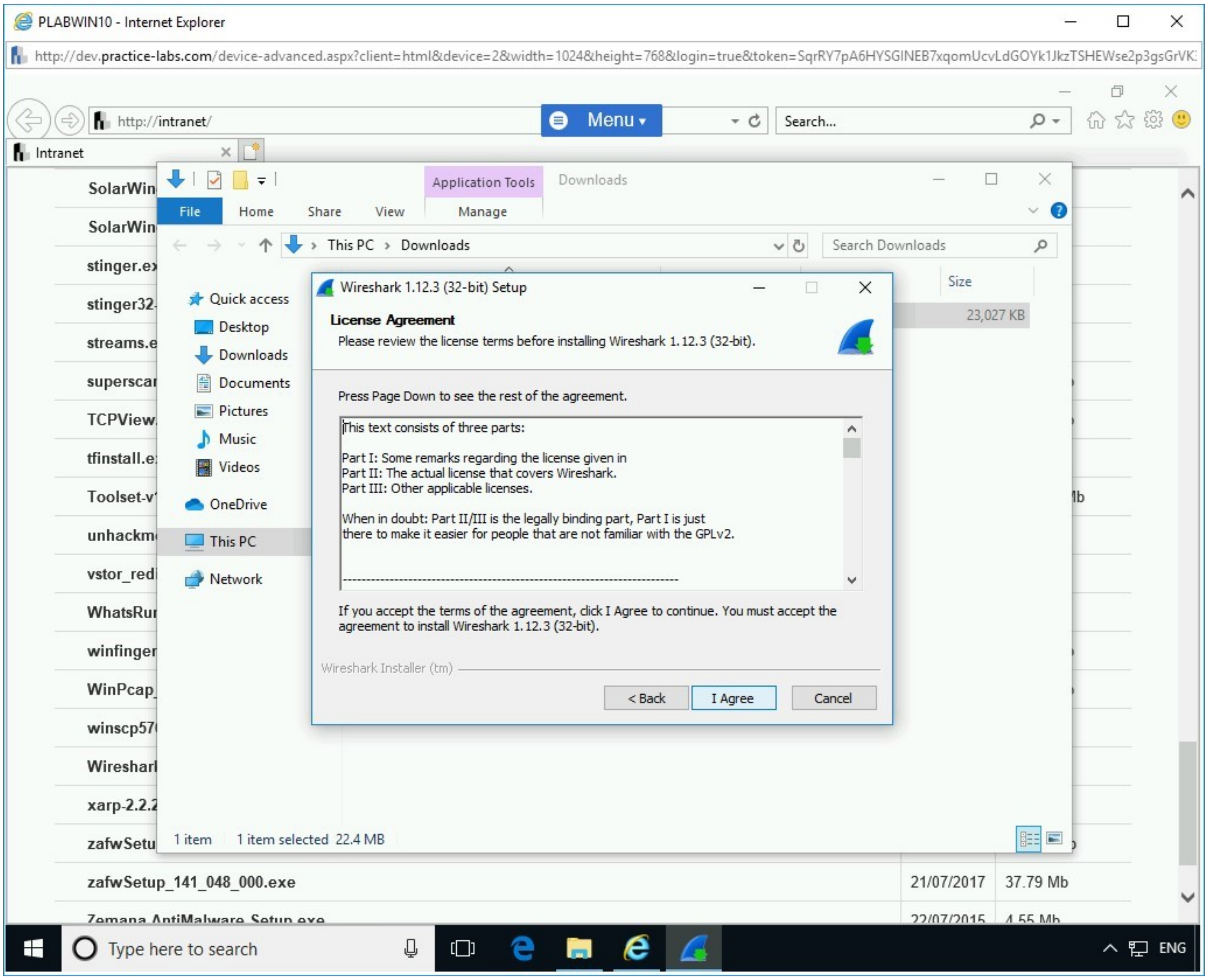
Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

Figure 1.53 Screenshot of PLABWIN10: Clicking Next on the Welcome to the Wireshark 1.12.3 (32-bit) Setup Wizard page.

Step 10

On the **License Agreement** page, click **I Agree**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
http://intranet/
Menu
Search...
Intranet
Application Tools
Downloads
File
Home
Share
View
Manage
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Size
23,027 KB
1 item 1 item selected 22.4 MB
zafwSetup_141_048_000.exe 21/07/2017 37.79 Mb
Type here to search
ENG
Wireshark 1.12.3 (32-bit) Setup
< Back
I Agree
Cancel

License Agreement

Please review the license terms before installing Wireshark 1.12.3 (32-bit).

Press Page Down to see the rest of the agreement.

This text consists of three parts:

Part I: Some remarks regarding the license given in
Part II: The actual license that covers Wireshark.
Part III: Other applicable licenses.

When in doubt: Part II/III is the legally binding part, Part I is just
there to make it easier for people that are not familiar with the GPLv2.

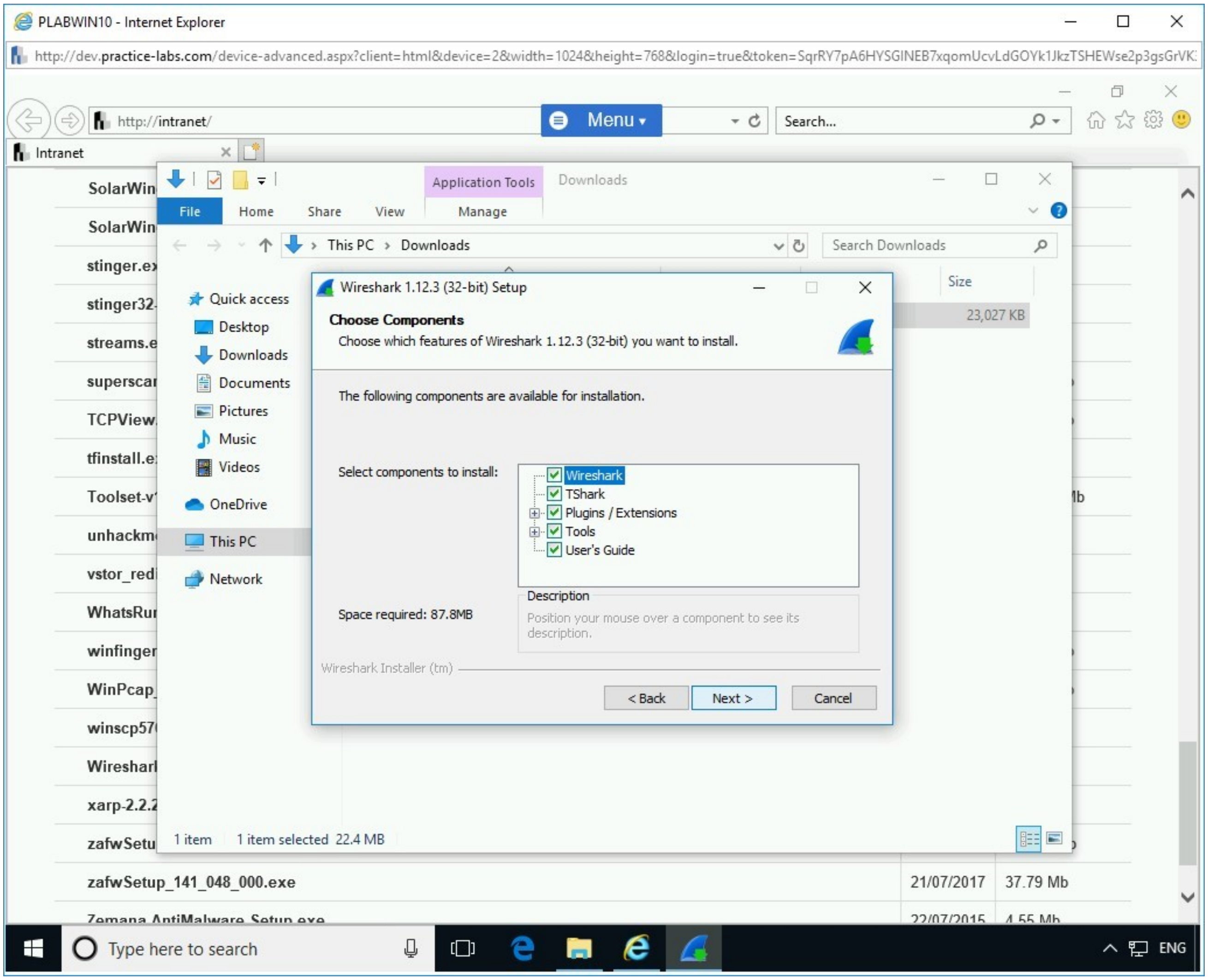
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 1.12.3 (32-bit).

Wireshark Installer (tm)

Figure 1.54 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 11

On the **Choose Components** page, keep the default selection and click **Next**.



Wireshark 1.12.3 (32-bit) Setup

Choose Components

Choose which features of Wireshark 1.12.3 (32-bit) you want to install.

The following components are available for installation.

Select components to install:

- ☑ Wireshark
- ☑ TShark
- ☑ Plugins / Extensions
- ☑ Tools
- ☑ User's Guide

Space required: 87.8MB

Description

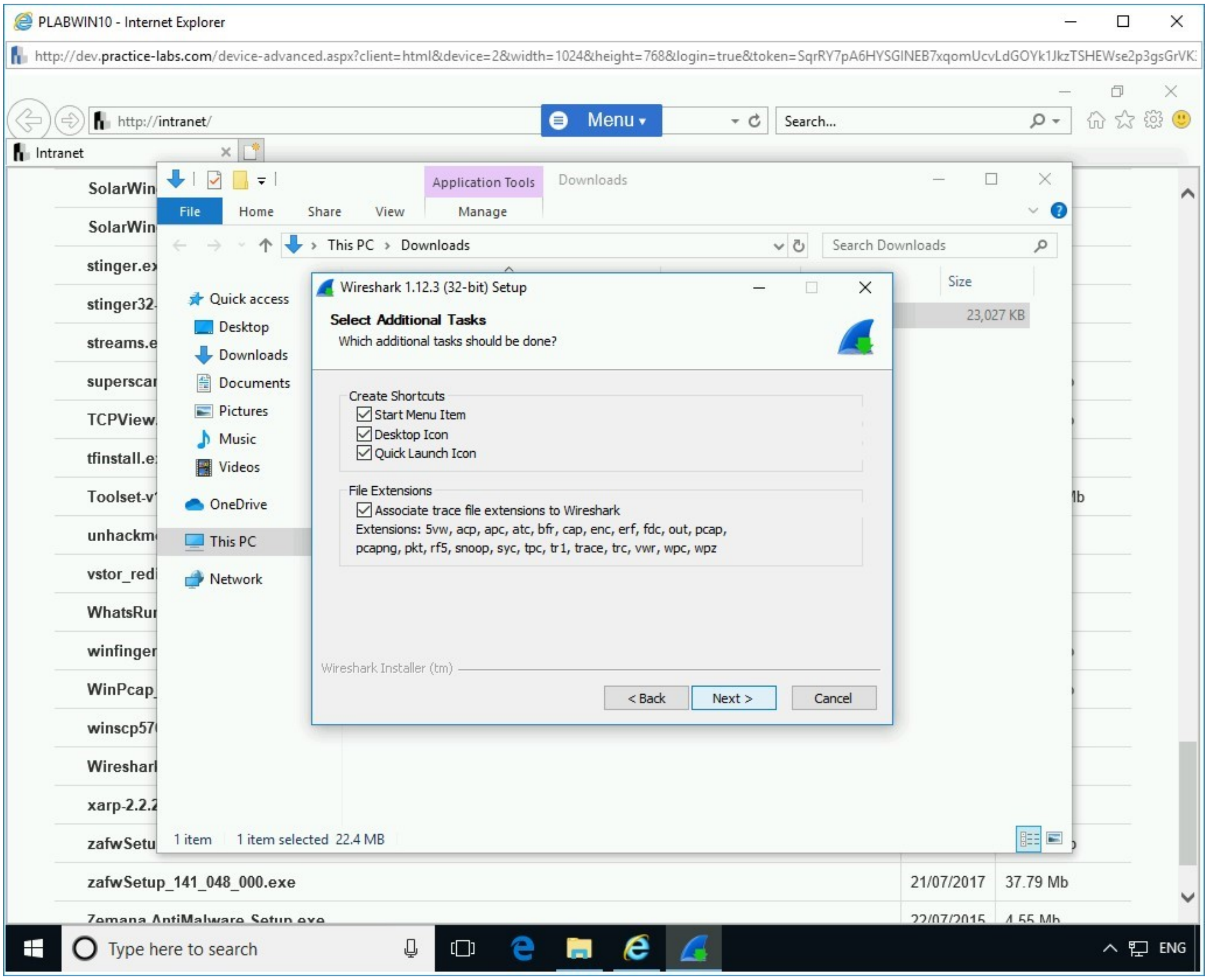
Position your mouse over a component to see its description.

Figure 1.55 Screenshot of PLABWIN10: Keeping the default options on the Choose Components page. Clicking Next.

Step 12

On the **Select Additional Tasks** page, select **Desktop** Icon.

Notice that the **Start Menu Item** and **Quick Launch Icons** options are already selected. Keep the option in the **File Extensions** section selected and click **Next**.



Wireshark 1.12.3 (32-bit) Setup

Select Additional Tasks

Which additional tasks should be done?

Create Shortcuts

☑ Start Menu Item
☑ Desktop Icon
☑ Quick Launch Icon

File Extensions

☑ Associate trace file extensions to Wireshark

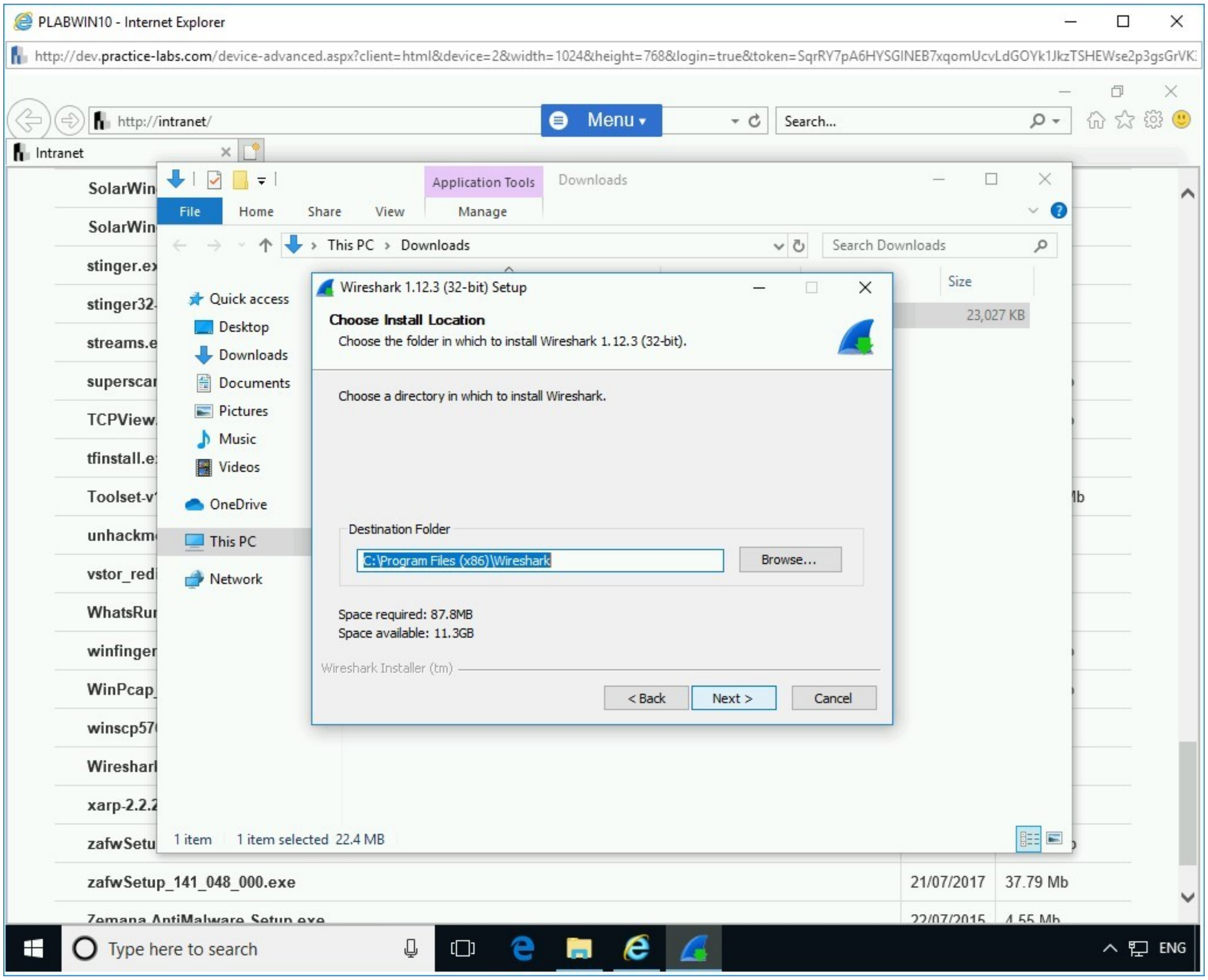
Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, out, pcap, pcapng, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz

Wireshark Installer (tm)

Figure 1.56 Screenshot of PLABWIN10: Selecting the Desktop Icon option on the Select Additional Tasks page. Clicking Next.

Step 13

On the **Choose Install Location** page, keep the default **Destination Folder** and click **Next**.



Wireshark 1.12.3 (32-bit) Setup

Choose Install Location

Choose the folder in which to install Wireshark 1.12.3 (32-bit).

Choose a directory in which to install Wireshark.

Destination Folder

C:\Program Files (x86)\Wireshark

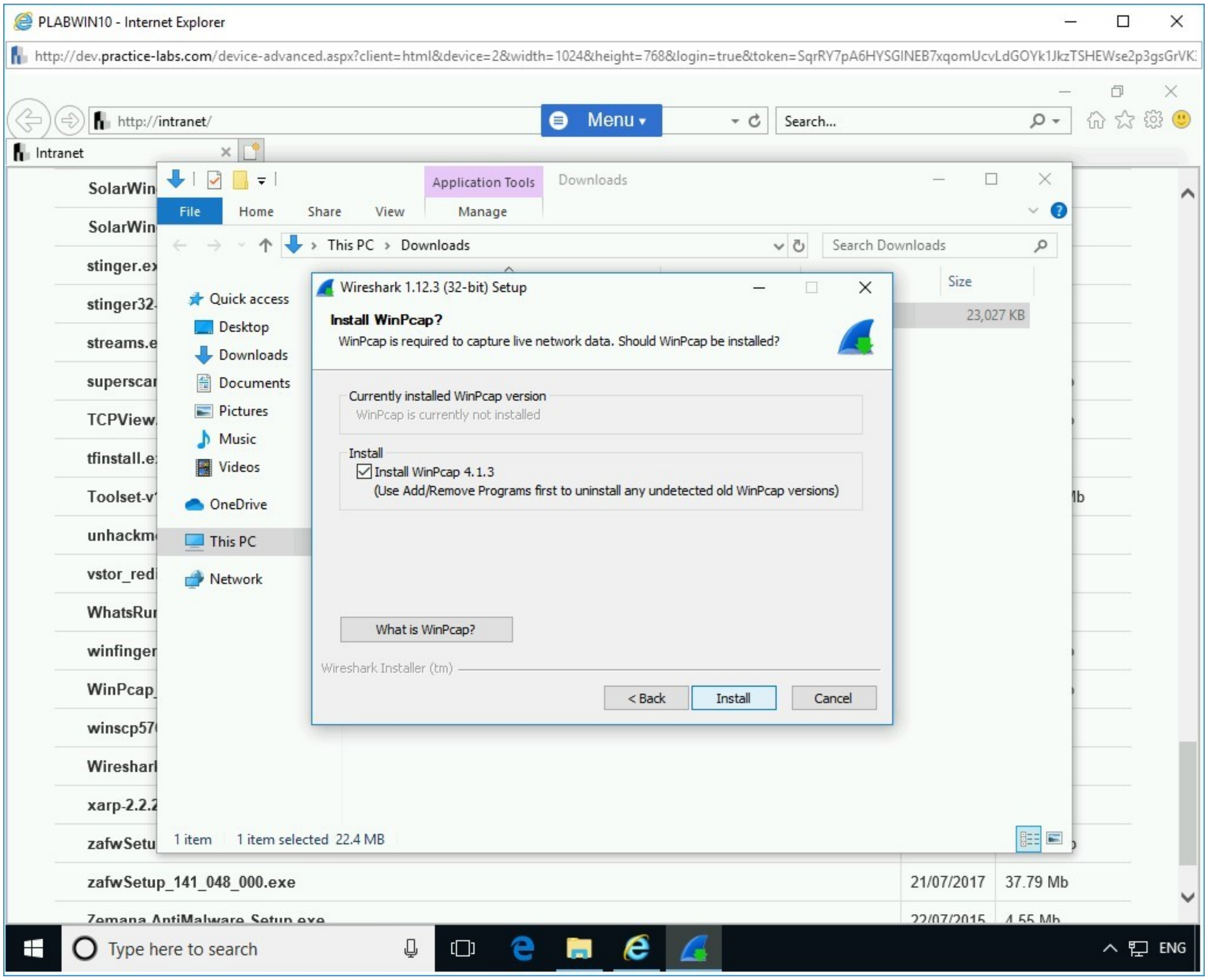
Space required: 87.8MB

Space available: 11.3GB

Figure 1.57 Screenshot of PLABWIN10: Keeping the default installation path on the Choose Install Location page. Clicking Next.

Step 14

On the **Install WinPcap?** page, keep the default selection and click **Install**.



Wireshark 1.12.3 (32-bit) Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version

WinPcap is currently not installed

Install

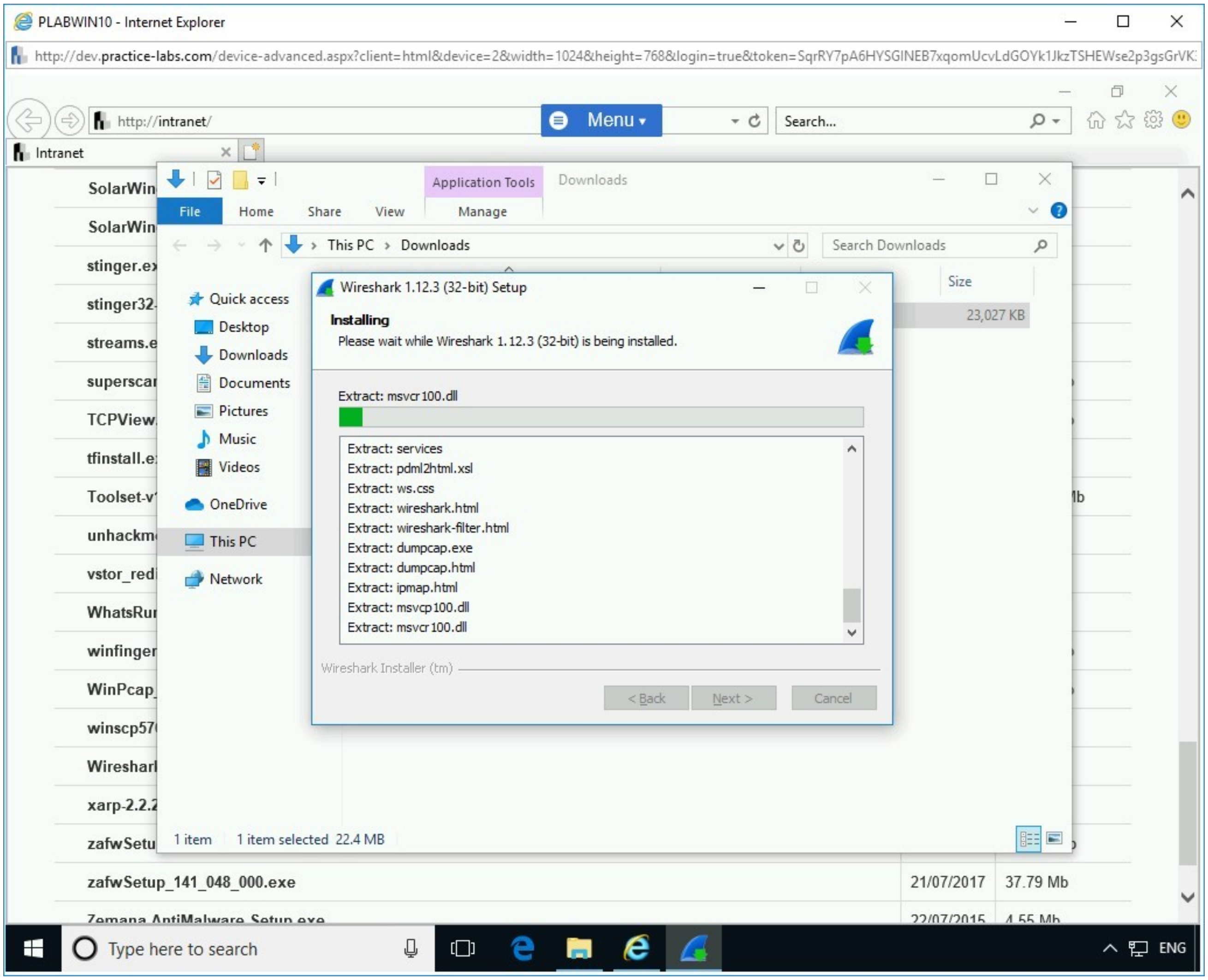
☑ Install WinPcap 4.1.3

(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)

Figure 1.58 Screenshot of PLABWIN10: Keeping the default installation option on the Install WinPcap? page. Clicking Install.

Step 15

On the **Installing** page, the installation process will start.



Wireshark 1.12.3 (32-bit) Setup

Installing

Please wait while Wireshark 1.12.3 (32-bit) is being installed.

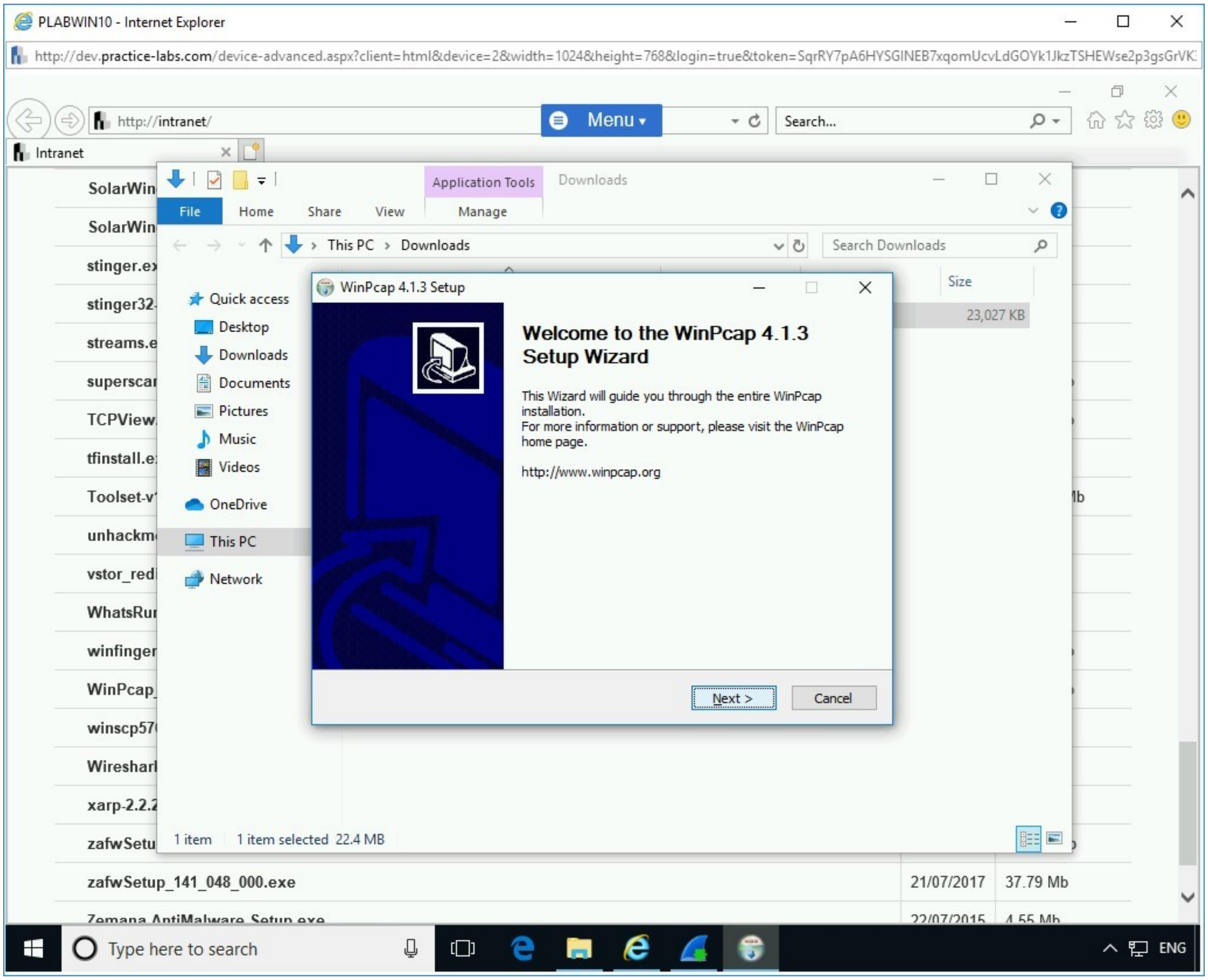
Extract: msvcr100.dll

```
Extract: services
Extract: pdml2html.xsl
Extract: ws.css
Extract: wireshark.html
Extract: wireshark-filter.html
Extract: dumpcap.exe
Extract: dumpcap.html
Extract: ipmap.html
Extract: msvcp100.dll
Extract: msvcr100.dll
```

Figure 1.59 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 16

On the **Welcome to the WinPcap 4.1.3 Setup Wizard** page, click **Next**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
http://intranet/
Menu
Search...
Intranet
Application Tools
Downloads
File
Home
Share
View
Manage
This PC > Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Size
23,027 KB
1 item 1 item selected 22.4 MB
WinPcap 4.1.3 Setup
Next >
Cancel
zafwSetup_141_048_000.exe 21/07/2017 37.79 Mb
Type here to search
ENG

Welcome to the WinPcap 4.1.3 Setup Wizard

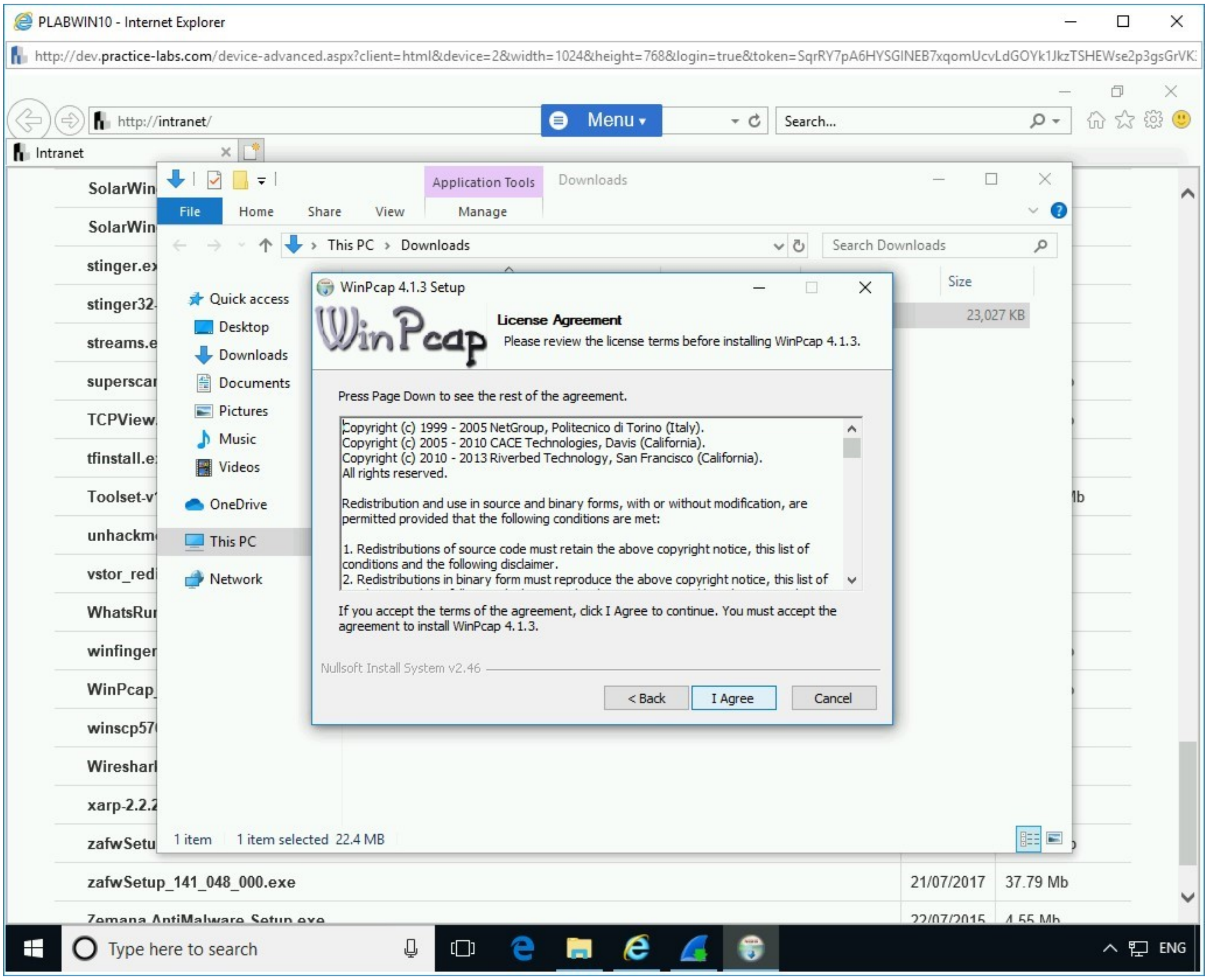
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

Figure 1.60 Screenshot of PLABWIN10: Clicking Next on the Welcome to the WinPcap 4.1.3 Setup Wizard page.

Step 17

On the **License Agreement** page, click **I Agree**.



License Agreement

Please review the license terms before installing WinPcap 4.1.3.

Press Page Down to see the rest of the agreement.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
Copyright (c) 2010 - 2013 Riverbed Technology, San Francisco (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

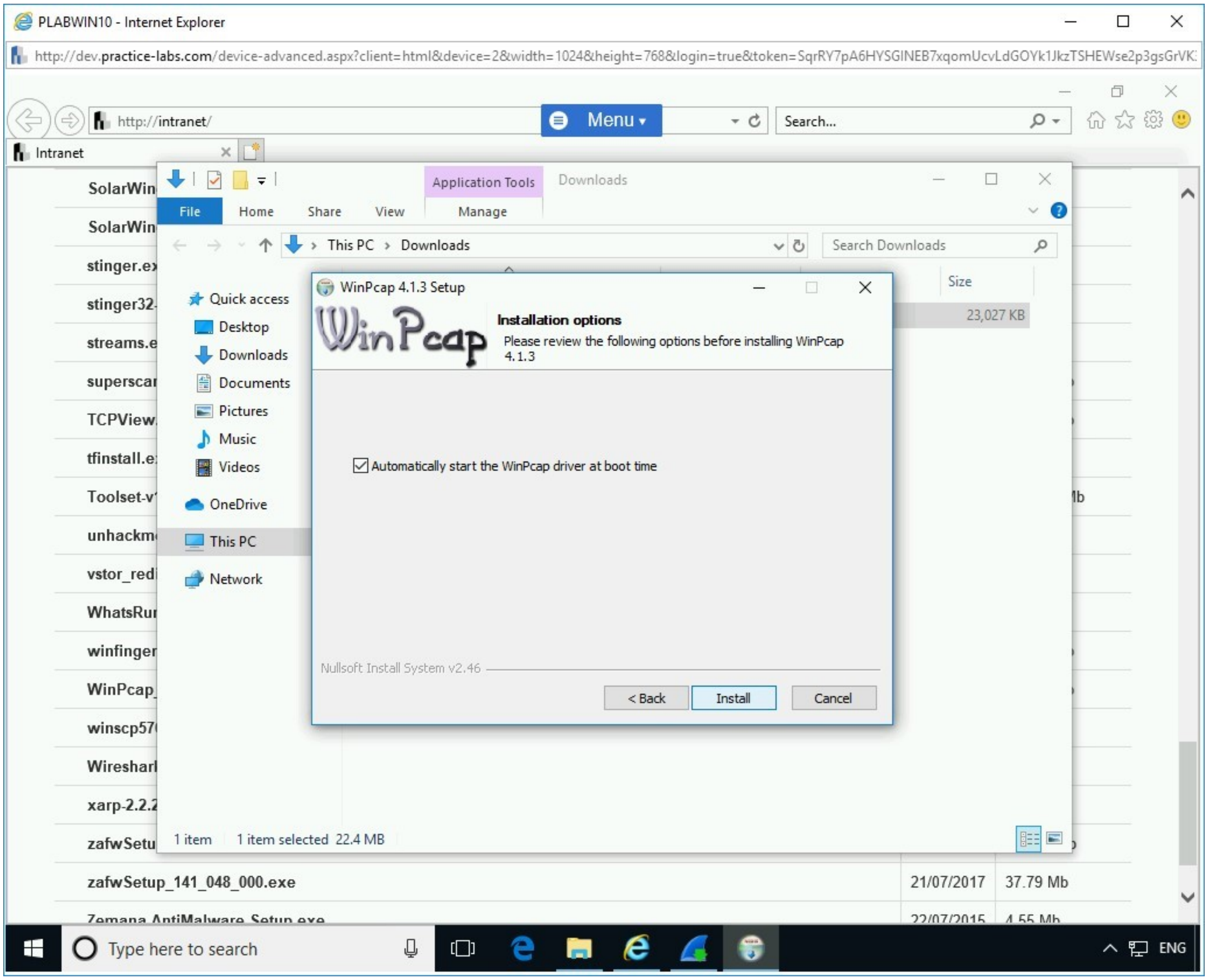
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.3.

Figure 1.61 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 18

On the **Installation Options** page, keep the default selection and click **Install**.



WinPcap 4.1.3 Setup

Installation options

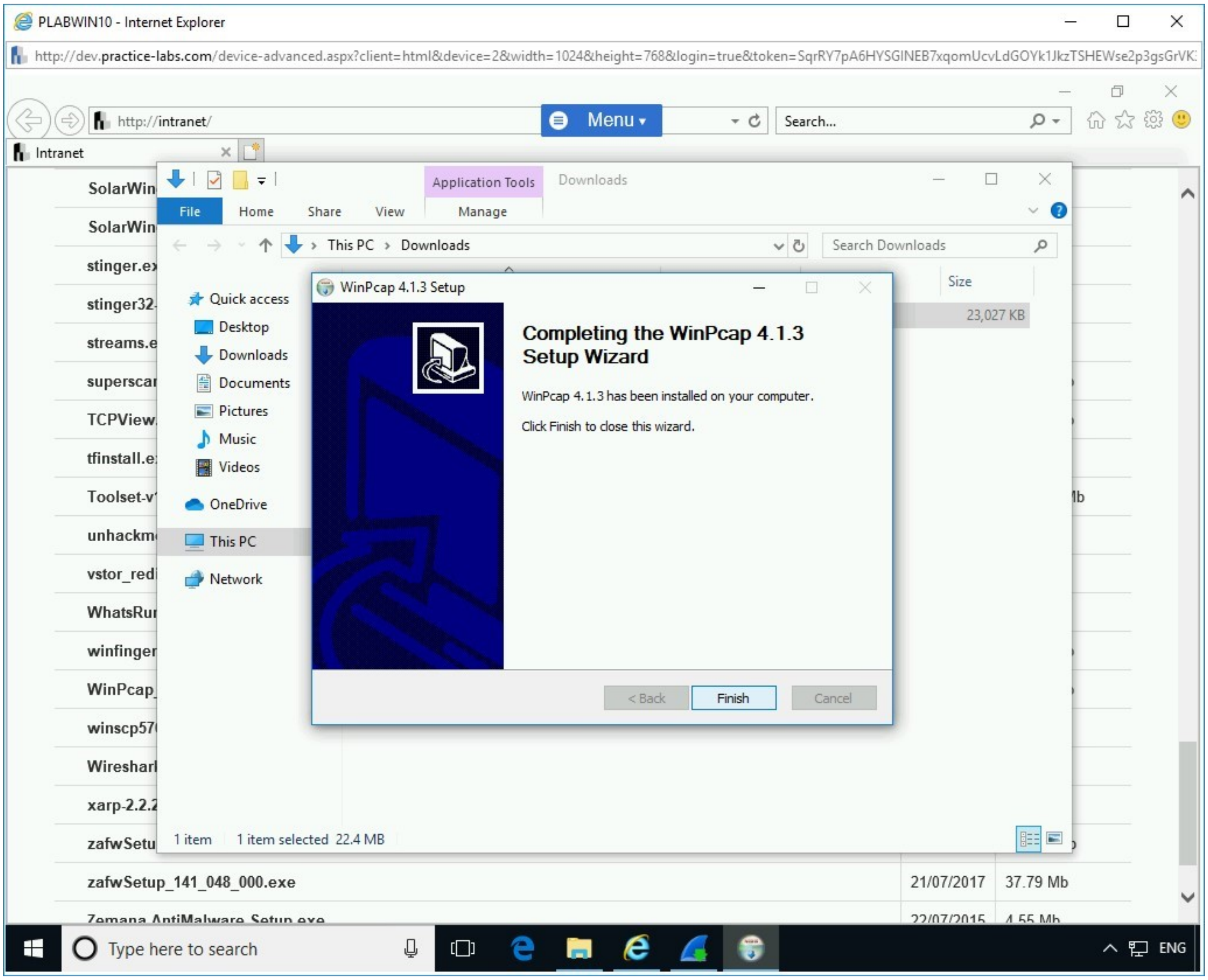
Please review the following options before installing WinPcap 4.1.3

☑ Automatically start the WinPcap driver at boot time

Figure 1.62 Screenshot of PLABWIN10: Keeping the default installation option on the Installation Options page. Clicking Install.

Step 19

On the **Completing the WinPcap 4.1.3 Setup Wizard** page, click **Finish**.



WinPcap 4.1.3 Setup

Completing the WinPcap 4.1.3 Setup Wizard

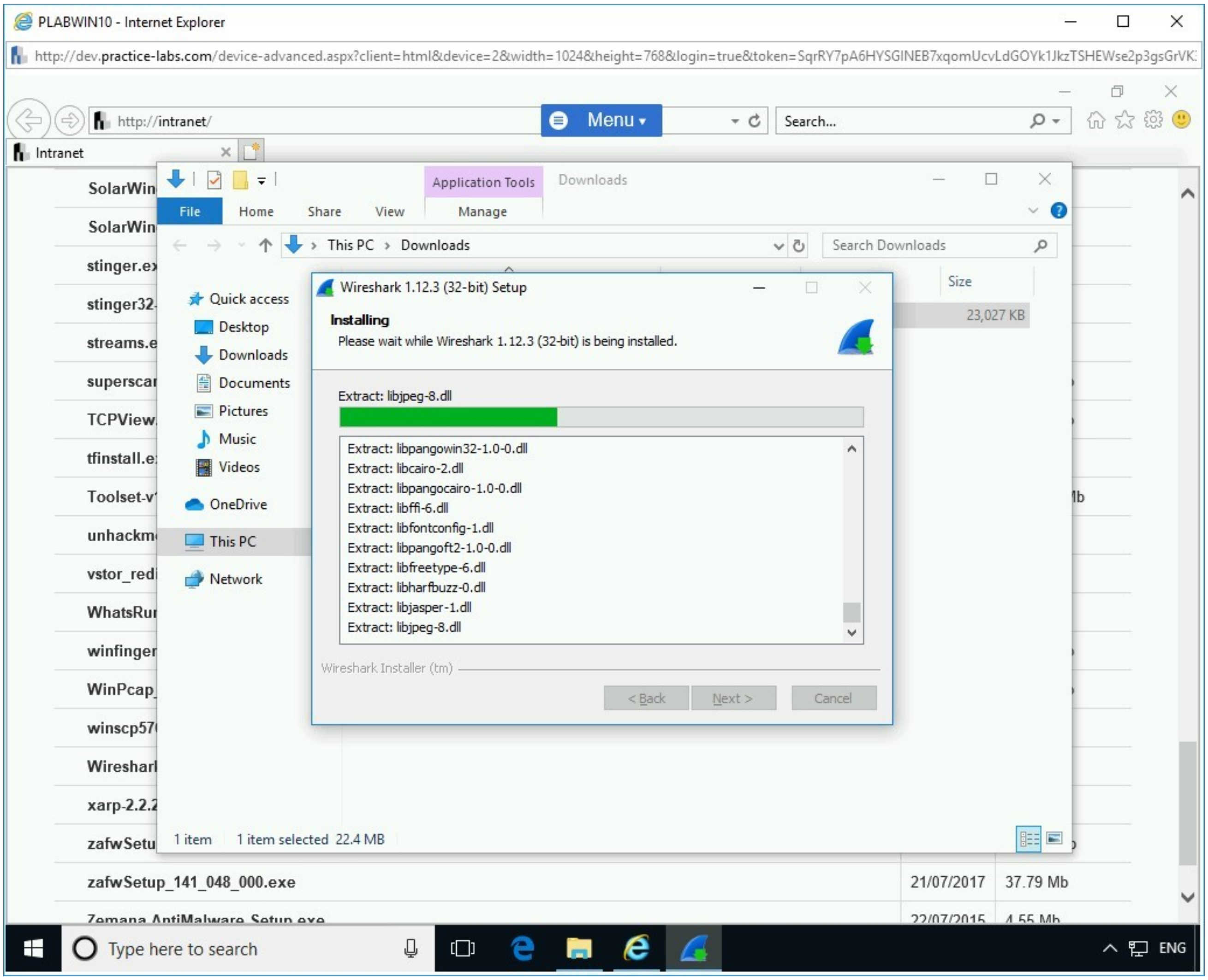
WinPcap 4.1.3 has been installed on your computer.

Click Finish to close this wizard.

Figure 1.63 Screenshot of PLABWIN10: Clicking Finish on the Completing the WinPcap 4.1.3 Setup Wizard page.

Step 20

On the **Installing** page, the installation progress is displayed.



Wireshark 1.12.3 (32-bit) Setup

Installing

Please wait while Wireshark 1.12.3 (32-bit) is being installed.

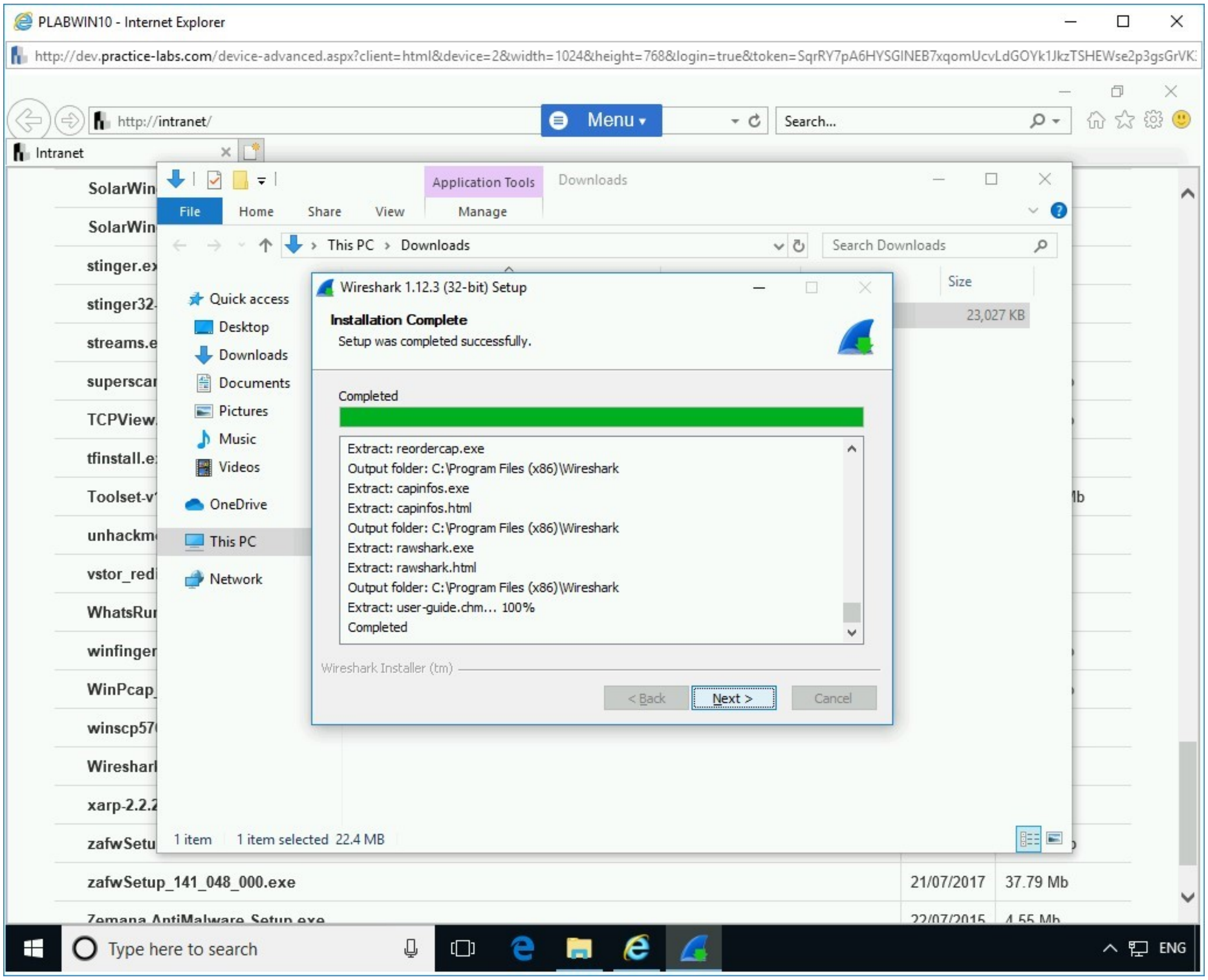
Extract: libjpeg-8.dll

```
Extract: libpangowin32-1.0-0.dll
Extract: libcairo-2.dll
Extract: libpangocairo-1.0-0.dll
Extract: libffi-6.dll
Extract: libfontconfig-1.dll
Extract: libpangoft2-1.0-0.dll
Extract: libfreetype-6.dll
Extract: libharfbuzz-0.dll
Extract: libjasper-1.dll
Extract: libjpeg-8.dll
```

Figure 1.64 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 21

On the **Installation Complete** page, click **Next**.



Installation Complete

Setup was completed successfully.

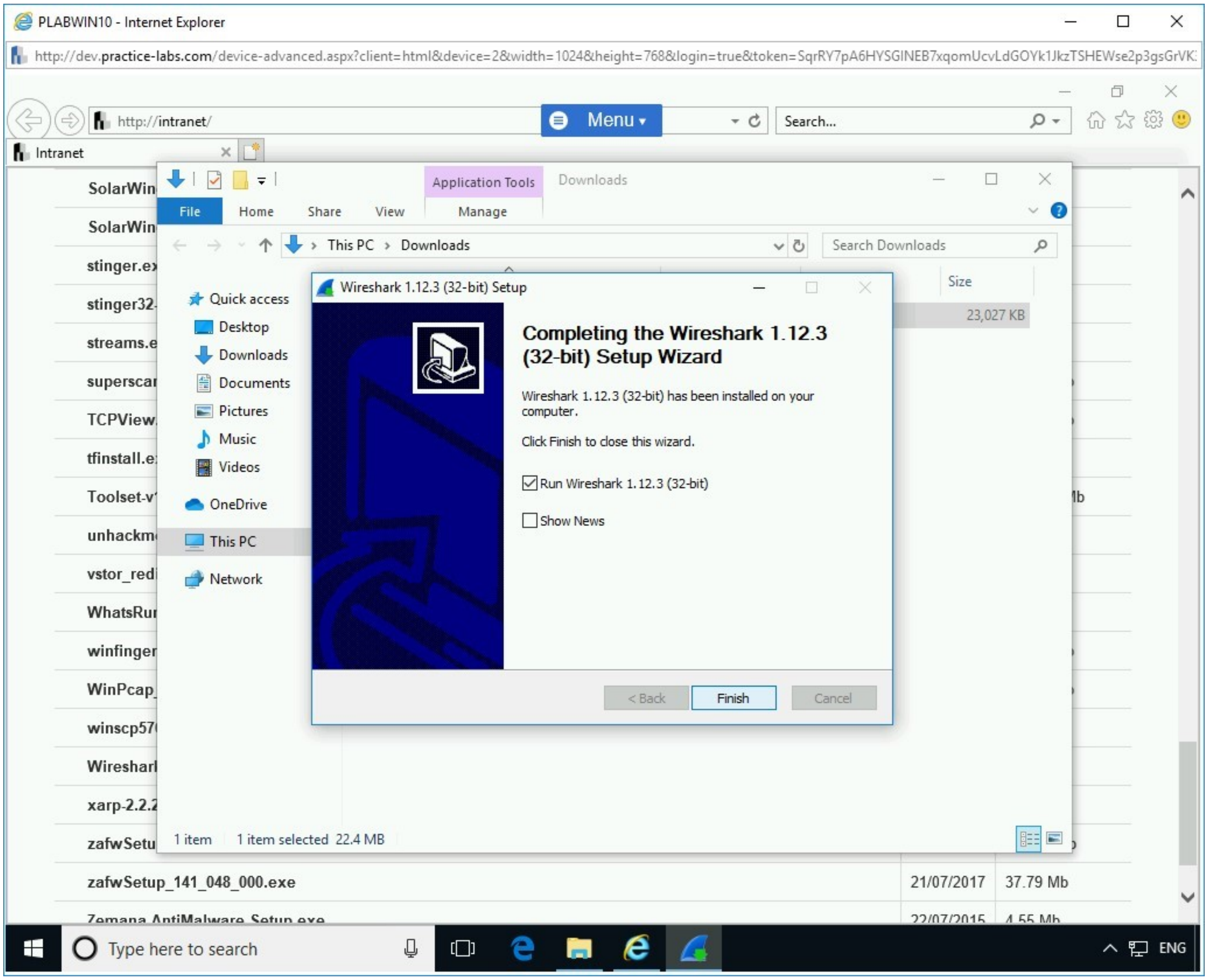
Completed

```
Extract: reordercap.exe
Output folder: C:\Program Files (x86)\Wireshark
Extract: capinfos.exe
Extract: capinfos.html
Output folder: C:\Program Files (x86)\Wireshark
Extract: rawshark.exe
Extract: rawshark.html
Output folder: C:\Program Files (x86)\Wireshark
Extract: user-guide.chm... 100%
Completed
```

Figure 1.65 Screenshot of PLABWIN10: Clicking Next on the Installation Complete page.

Step 22

On the **Completing the Wireshark 1.12.3 (32-bit) Setup Wizard** page, **select Run Wireshark 1.12.3 (32-bit)** and click **Finish**.



Wireshark 1.12.3 (32-bit) Setup

Completing the Wireshark 1.12.3 (32-bit) Setup Wizard

Wireshark 1.12.3 (32-bit) has been installed on your computer.

Click Finish to close this wizard.

☑ Run Wireshark 1.12.3 (32-bit)

☐ Show News

Figure 1.66 Screenshot of PLABWIN10: Run Wireshark 1.12.3 (32-bit) selected. Clicking Finish on the Completing the Wireshark 1.12.3 (32-bit) Setup Wizard page.

Step 23

The **Wireshark** window is displayed. The **Software Update** dialog box is also displayed. Click **Remind me later**.

You are now on the **Wireshark** window.

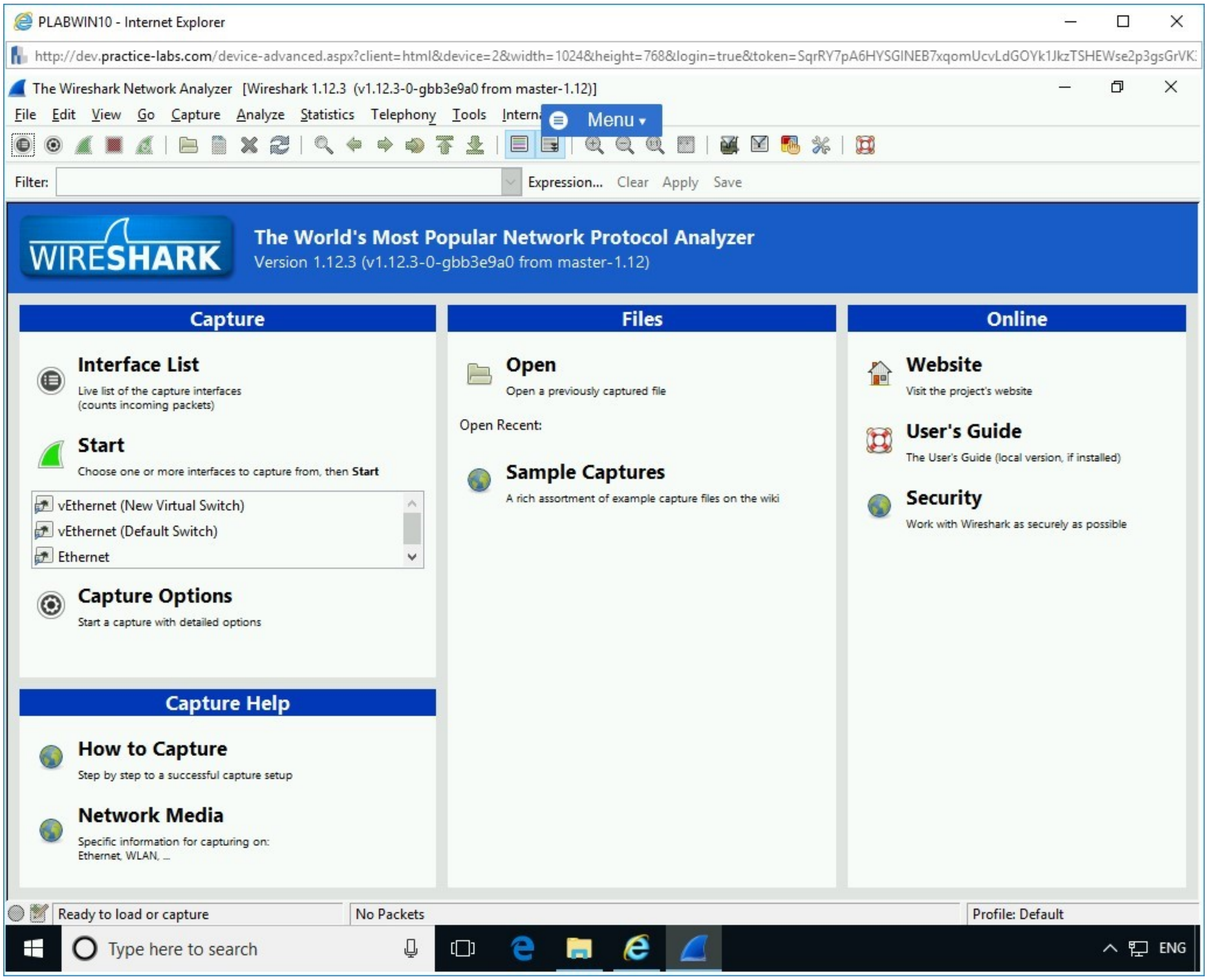
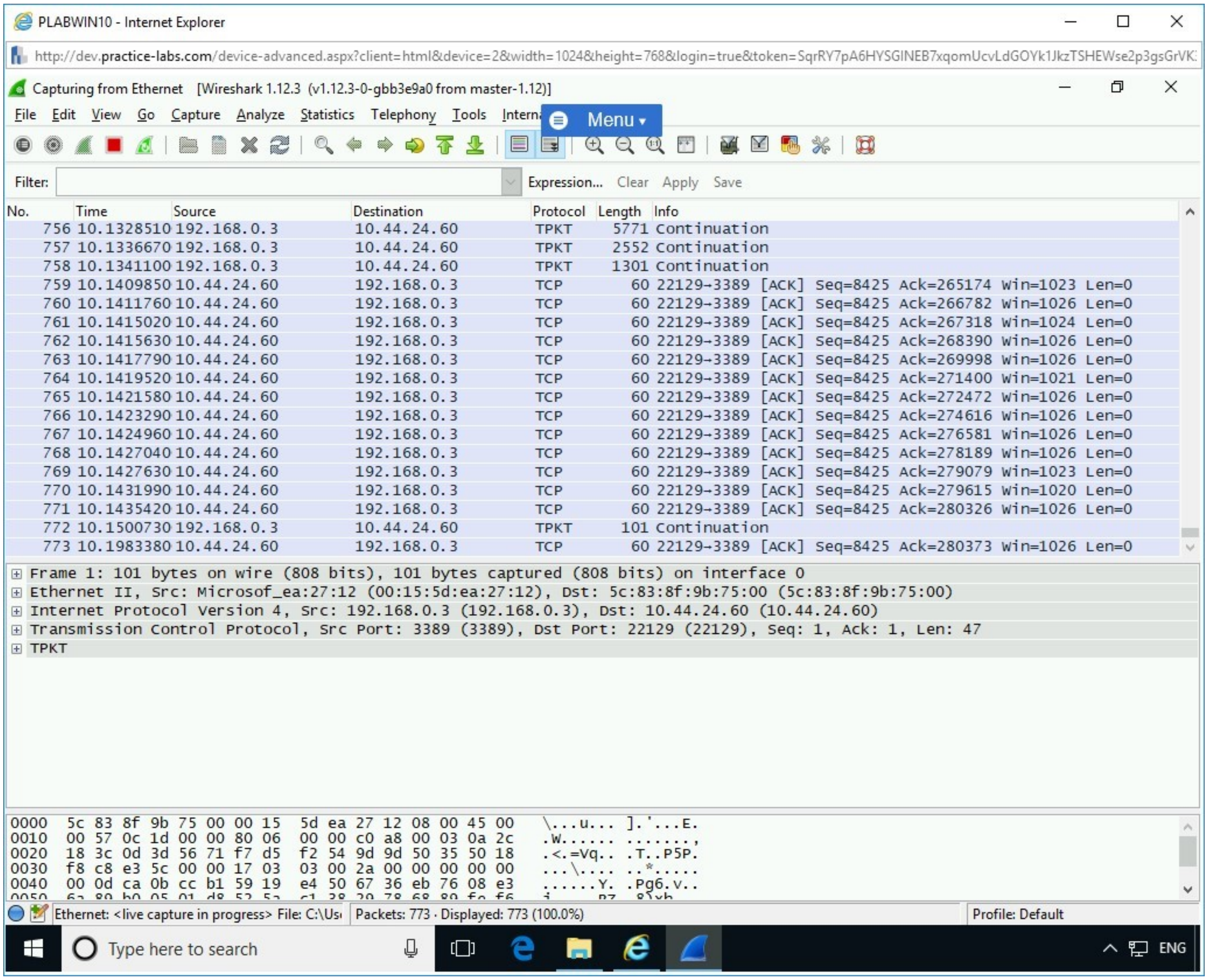

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK:
The Wireshark Network Analyzer [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Intern
Menu
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
vEthernet (New Virtual Switch)
vEthernet (Default Switch)
Ethernet
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Ready to load or capture
No Packets
Profile: Default
Type here to search
ENG

Figure 1.67 Screenshot of PLABWIN10: Showing the Wireshark window.

Step 24

Maximise the window, select **Ethernet** and click **Start**. Notice that packet capturing starts.

Close the **File Explorer** & **Internet Explorer** windows.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=SqrRY7pA6HYSGINEB7xqomUcvLdGOYk1JkzTSHEWse2p3gsGrVK
Capturing from Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Intern
Menu
Filter:
Expression... Clear Apply Save

```
No.   Time       Source         Destination    Protocol Length Info
  756 10.1328510 192.168.0.3    10.44.24.60    TPKT     5771 Continuation
  757 10.1336670 192.168.0.3    10.44.24.60    TPKT     2552 Continuation
  758 10.1341100 192.168.0.3    10.44.24.60    TPKT     1301 Continuation
  759 10.1409850 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=265174 Win=1023 Len=0
  760 10.1411760 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=266782 Win=1026 Len=0
  761 10.1415020 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=267318 Win=1024 Len=0
  762 10.1415630 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=268390 Win=1026 Len=0
  763 10.1417790 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=269998 Win=1026 Len=0
  764 10.1419520 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=271400 Win=1021 Len=0
  765 10.1421580 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=272472 Win=1026 Len=0
  766 10.1423290 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=274616 Win=1026 Len=0
  767 10.1424960 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=276581 Win=1026 Len=0
  768 10.1427040 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=278189 Win=1026 Len=0
  769 10.1427630 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=279079 Win=1023 Len=0
  770 10.1431990 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=279615 Win=1020 Len=0
  771 10.1435420 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=280326 Win=1026 Len=0
  772 10.1500730 192.168.0.3    10.44.24.60    TPKT      101 Continuation
  773 10.1983380 10.44.24.60    192.168.0.3    TCP        60 22129→3389 [ACK] Seq=8425 Ack=280373 Win=1026 Len=0
```

```
⊞ Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 22129 (22129), Seq: 1, Ack: 1, Len: 47
⊞ TPKT
```

```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 0c 1d 00 00 80 06  00 00 c0 a8 00 03 0a 2c   .W...... .......,
0020  18 3c 0d 3d 56 71 f7 d5  f2 54 9d 9d 50 35 50 18   .<.=Vq.. .T..P5P.
0030  f8 c8 e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 0d ca 0b cc b1 59 19  e4 50 67 36 eb 76 08 e3   ......Y. .Pg6.v..
```

Ethernet: <live capture in progress> File: C:\Us
Packets: 773 · Displayed: 773 (100.0%)
Profile: Default
Type here to search
ENG

Figure 1.68 Screenshot of PLABWIN10: Showing the packet capture progress in Wireshark.

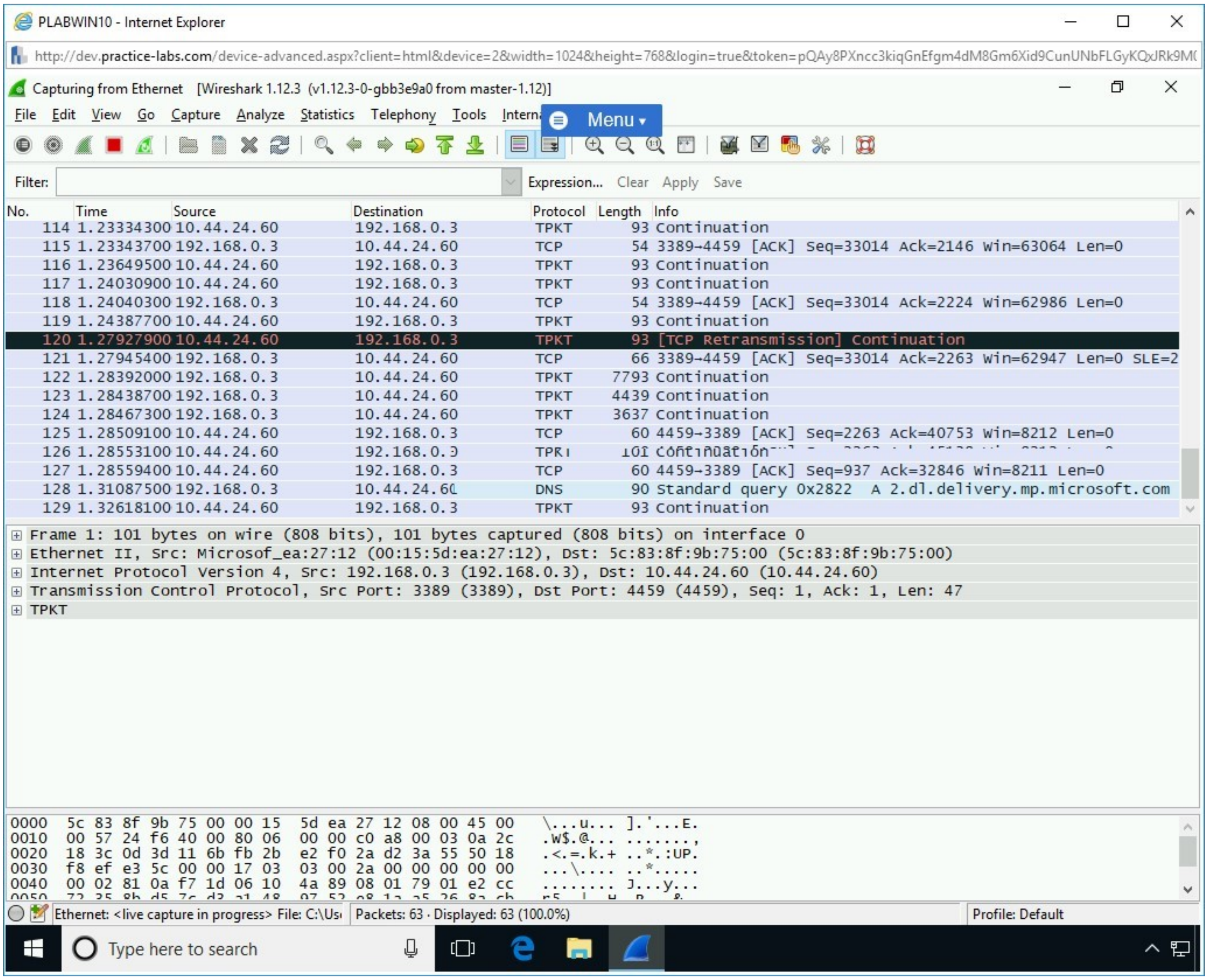
Task 4 - Use Wireshark

In this task, you will learn to use Wireshark. To use Wireshark, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**.

The **Wireshark Network Analyzer** window is displayed.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
Capturing from Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Interna
Menu ▾
Filter:
Expression... Clear Apply Save
Profile: Default
Type here to search

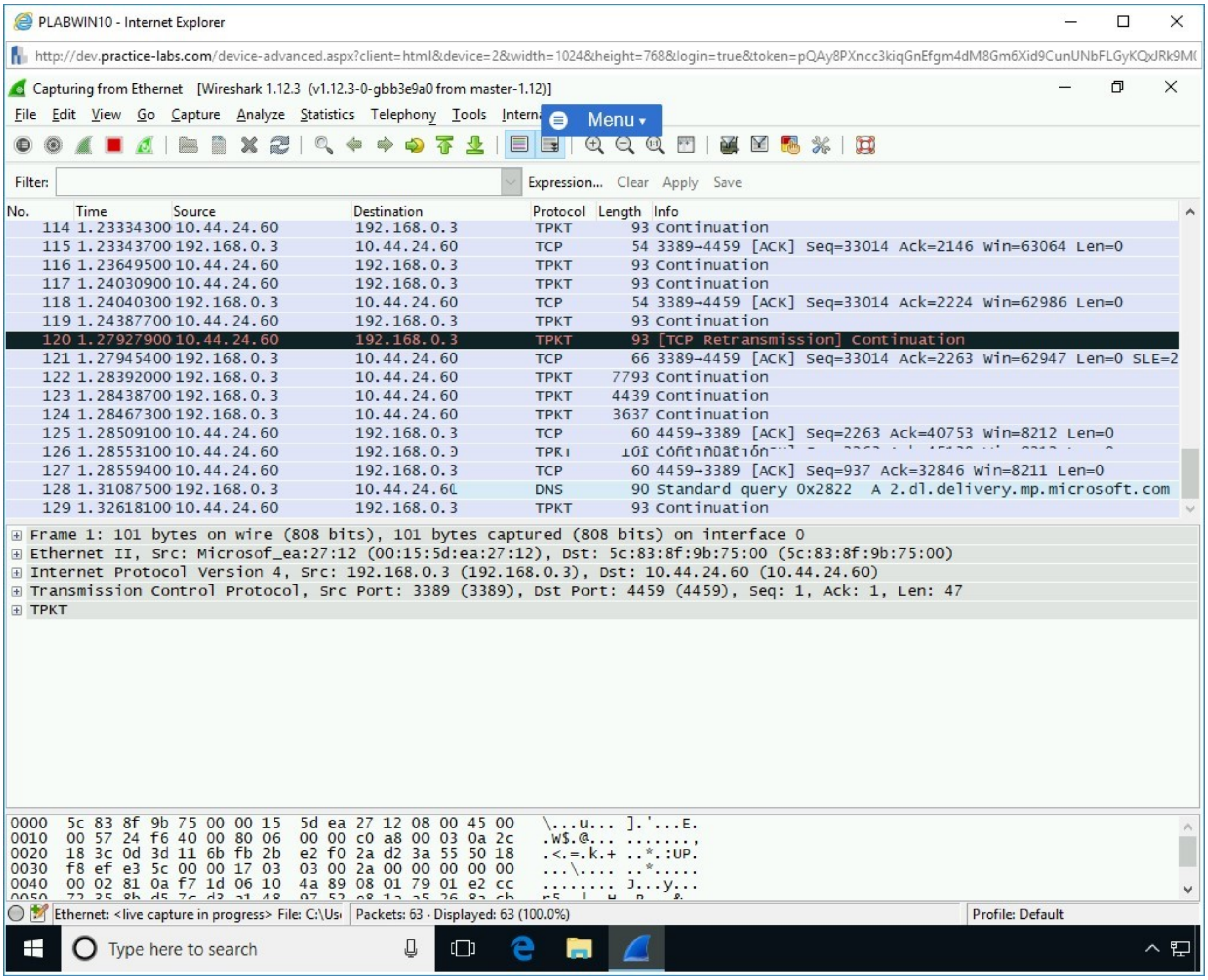
```
No.   Time       Source       Destination   Protocol Length Info
  114 1.23334300 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  115 1.23343700 192.168.0.3  10.44.24.60   TCP        54 3389→4459 [ACK] Seq=33014 Ack=2146 Win=63064 Len=0
  116 1.23649500 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  117 1.24030900 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  118 1.24040300 192.168.0.3  10.44.24.60   TCP        54 3389→4459 [ACK] Seq=33014 Ack=2224 Win=62986 Len=0
  119 1.24387700 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  120 1.27927900 10.44.24.60  192.168.0.3   TPKT       93 [TCP Retransmission] Continuation
  121 1.27945400 192.168.0.3  10.44.24.60   TCP        66 3389→4459 [ACK] Seq=33014 Ack=2263 Win=62947 Len=0 SLE=2
  122 1.28392000 192.168.0.3  10.44.24.60   TPKT     7793 Continuation
  123 1.28438700 192.168.0.3  10.44.24.60   TPKT     4439 Continuation
  124 1.28467300 192.168.0.3  10.44.24.60   TPKT     3637 Continuation
  125 1.28509100 10.44.24.60  192.168.0.3   TCP        60 4459→3389 [ACK] Seq=2263 Ack=40753 Win=8212 Len=0
  126 1.28553100 10.44.24.60  192.168.0.3   TPKT      101 Continuation
  127 1.28559400 10.44.24.60  192.168.0.3   TCP        60 4459→3389 [ACK] Seq=937 Ack=32846 Win=8211 Len=0
  128 1.31087500 192.168.0.3  10.44.24.60   DNS        90 Standard query 0x2822  A 2.dl.delivery.mp.microsoft.com
  129 1.32618100 10.44.24.60  192.168.0.3   TPKT       93 Continuation

⊞ Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 4459 (4459), Seq: 1, Ack: 1, Len: 47
⊞ TPKT

0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 24 f6 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .W$.@... .......,
0020  18 3c 0d 3d 11 6b fb 2b  e2 f0 2a d2 3a 55 50 18   .<.=.k.+ ..*.:UP.
0030  f8 ef e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 02 81 0a f7 1d 06 10  4a 89 08 01 79 01 e2 cc   ........ J...y...

Ethernet: <live capture in progress> File: C:\Us   Packets: 63 · Displayed: 63 (100.0%)
```

Figure 1.69 Screenshot of PLABWIN10: Showing the packet capture progress in Wireshark.

Step 2

The **Capturing from Ethernet** window is displayed.

Note that there are several packets being analyzed.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
Capturing from Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Interna
Menu
Filter:
Expression... Clear Apply Save
Type here to search

```
No.   Time       Source       Destination   Protocol Length Info
  114 1.23334300 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  115 1.23343700 192.168.0.3  10.44.24.60   TCP        54 3389→4459 [ACK] Seq=33014 Ack=2146 Win=63064 Len=0
  116 1.23649500 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  117 1.24030900 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  118 1.24040300 192.168.0.3  10.44.24.60   TCP        54 3389→4459 [ACK] Seq=33014 Ack=2224 Win=62986 Len=0
  119 1.24387700 10.44.24.60  192.168.0.3   TPKT       93 Continuation
  120 1.27927900 10.44.24.60  192.168.0.3   TPKT       93 [TCP Retransmission] Continuation
  121 1.27945400 192.168.0.3  10.44.24.60   TCP        66 3389→4459 [ACK] Seq=33014 Ack=2263 Win=62947 Len=0 SLE=2
  122 1.28392000 192.168.0.3  10.44.24.60   TPKT     7793 Continuation
  123 1.28438700 192.168.0.3  10.44.24.60   TPKT     4439 Continuation
  124 1.28467300 192.168.0.3  10.44.24.60   TPKT     3637 Continuation
  125 1.28509100 10.44.24.60  192.168.0.3   TCP        60 4459→3389 [ACK] Seq=2263 Ack=40753 Win=8212 Len=0
  126 1.28553100 10.44.24.60  192.168.0.3   TPKT      101 Continuation
  127 1.28559400 10.44.24.60  192.168.0.3   TCP        60 4459→3389 [ACK] Seq=937 Ack=32846 Win=8211 Len=0
  128 1.31087500 192.168.0.3  10.44.24.60   DNS        90 Standard query 0x2822  A 2.dl.delivery.mp.microsoft.com
  129 1.32618100 10.44.24.60  192.168.0.3   TPKT       93 Continuation
```

```
⊞ Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 4459 (4459), Seq: 1, Ack: 1, Len: 47
⊞ TPKT
```

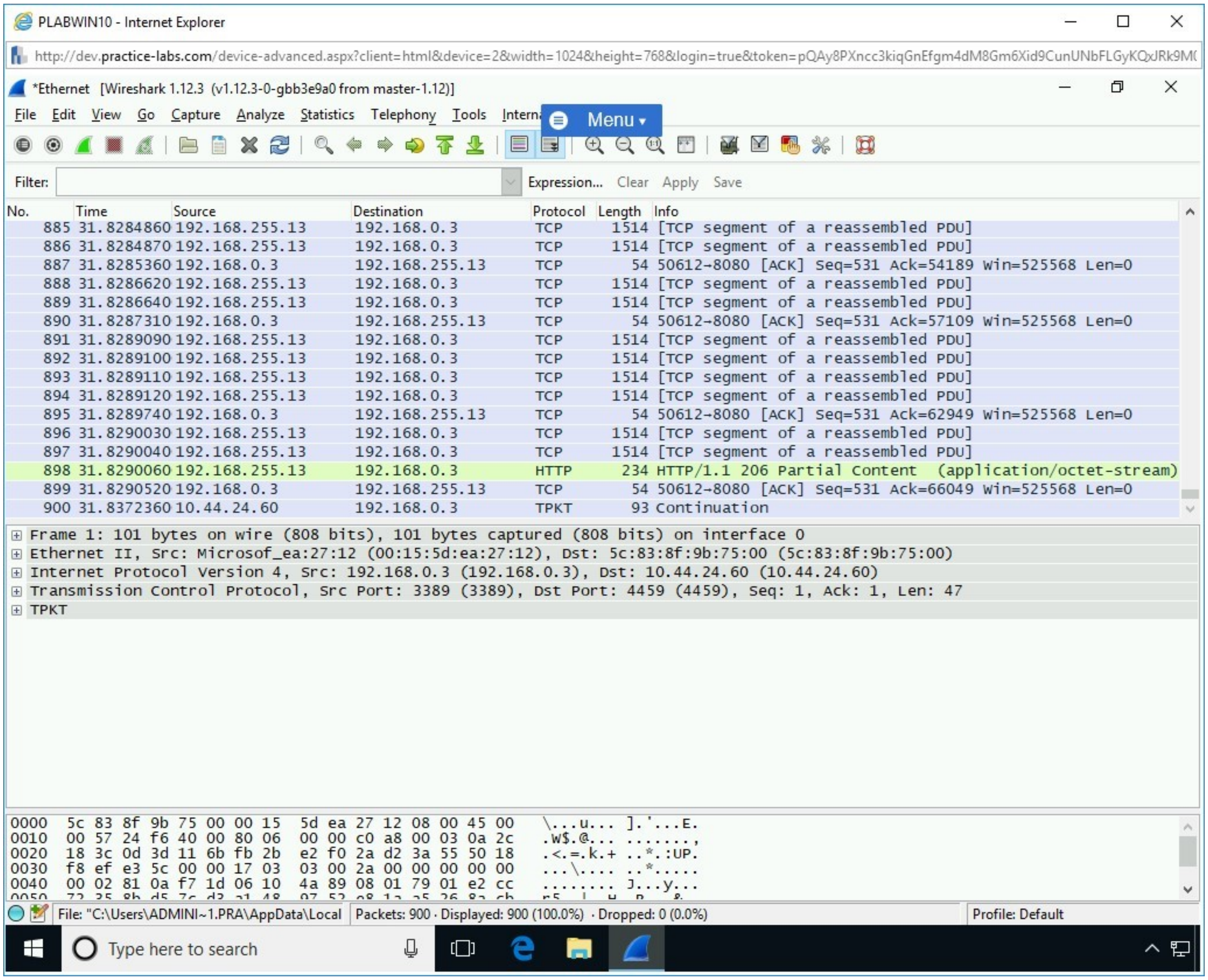
```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 24 f6 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .W$.@... .......,
0020  18 3c 0d 3d 11 6b fb 2b  e2 f0 2a d2 3a 55 50 18   .<.=.k.+ ..*.:UP.
0030  f8 ef e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 02 81 0a f7 1d 06 10  4a 89 08 01 79 01 e2 cc   ........ J...y...
```

Ethernet: <live capture in progress> File: C:\Us Packets: 63 · Displayed: 63 (100.0%) Profile: Default

Figure 1.70 Screenshot of PLABWIN10: Showing the packet capture analyzing packets in Wireshark.

Step 3

Click **Stop** (the red square icon, found at the top left of the window). This will end the packet capture.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M
*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Interna
Menu ▾
Filter:
Expression... Clear Apply Save
Type here to search

```
No.    Time       Source          Destination      Protocol Length Info
   885 31.8284860 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   886 31.8284870 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   887 31.8285360 192.168.0.3     192.168.255.13   TCP        54 50612→8080 [ACK] Seq=531 Ack=54189 Win=525568 Len=0
   888 31.8286620 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   889 31.8286640 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   890 31.8287310 192.168.0.3     192.168.255.13   TCP        54 50612→8080 [ACK] Seq=531 Ack=57109 Win=525568 Len=0
   891 31.8289090 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   892 31.8289100 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   893 31.8289110 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   894 31.8289120 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   895 31.8289740 192.168.0.3     192.168.255.13   TCP        54 50612→8080 [ACK] Seq=531 Ack=62949 Win=525568 Len=0
   896 31.8290030 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   897 31.8290040 192.168.255.13  192.168.0.3      TCP      1514 [TCP segment of a reassembled PDU]
   898 31.8290060 192.168.255.13  192.168.0.3      HTTP      234 HTTP/1.1 206 Partial Content  (application/octet-stream)
   899 31.8290520 192.168.0.3     192.168.255.13   TCP        54 50612→8080 [ACK] Seq=531 Ack=66049 Win=525568 Len=0
   900 31.8372360 10.44.24.60     192.168.0.3      TPKT       93 Continuation
```

```
⊞ Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 4459 (4459), Seq: 1, Ack: 1, Len: 47
⊞ TPKT
```

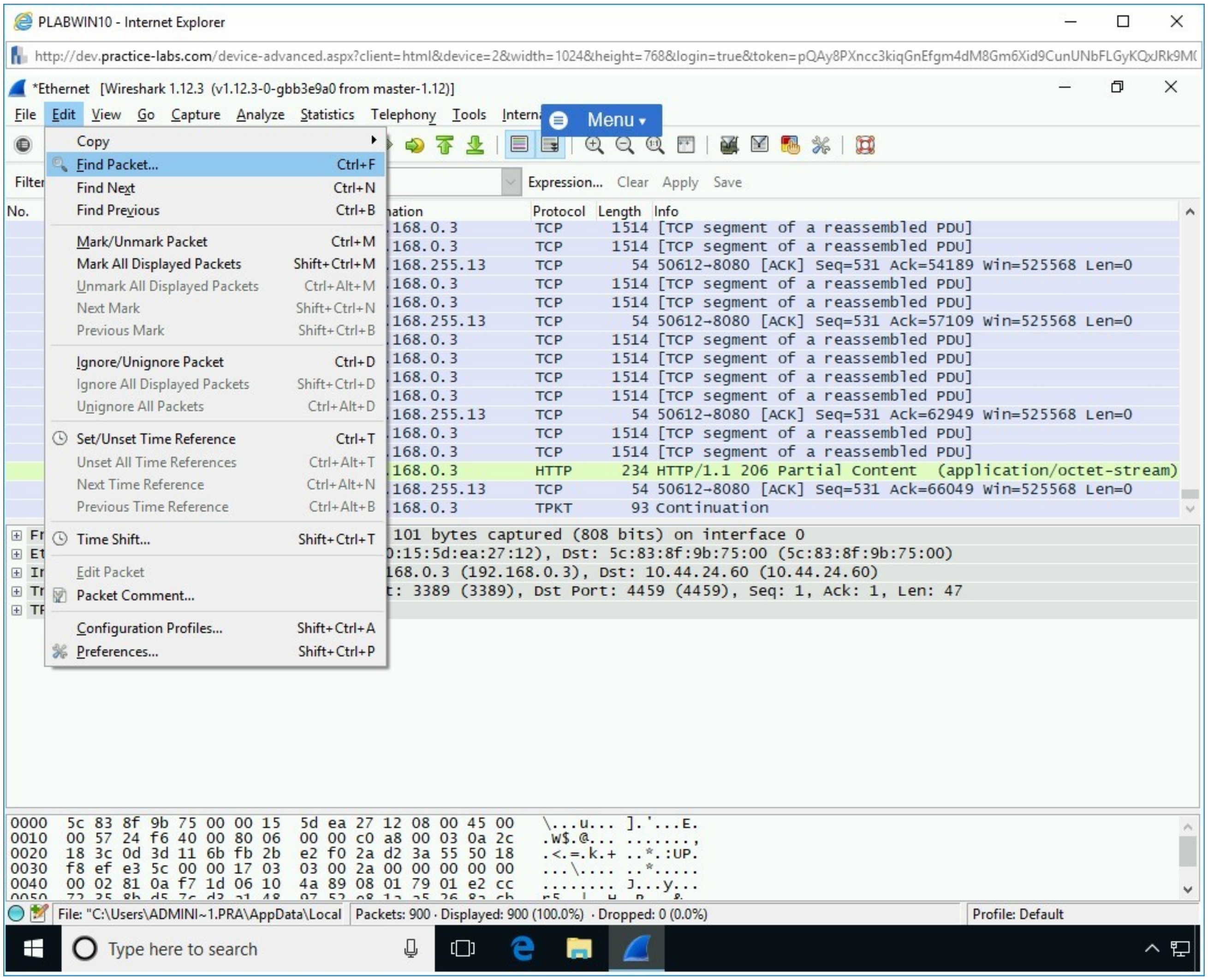
```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 24 f6 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .W$.@... .......,
0020  18 3c 0d 3d 11 6b fb 2b  e2 f0 2a d2 3a 55 50 18   .<.=.k.+ ..*.:UP.
0030  f8 ef e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 02 81 0a f7 1d 06 10  4a 89 08 01 79 01 e2 cc   ........ J...y...
```

File: "C:\Users\ADMINI~1.PRA\AppData\Local | Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Figure 1.71 Screenshot of PLABWIN10: Showing the stopped packet capturing in Wireshark.

Step 5

Click **Edit** and then select **Find Packet**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Intern
Menu ▾
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Packets Shift+Ctrl+M
Unmark All Displayed Packets Ctrl+Alt+M
Next Mark Shift+Ctrl+N
Previous Mark Shift+Ctrl+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Packets Shift+Ctrl+D
Unignore All Packets Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Shift+Ctrl+T
Edit Packet
Packet Comment...
Configuration Profiles... Shift+Ctrl+A
Preferences... Shift+Ctrl+P
Filter
Expression...
Clear
Apply
Save
No.
Type here to search
Profile: Default

```
ation          Protocol Length Info
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.255.13    TCP        54 50612→8080 [ACK] Seq=531 Ack=54189 Win=525568 Len=0
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.255.13    TCP        54 50612→8080 [ACK] Seq=531 Ack=57109 Win=525568 Len=0
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.255.13    TCP        54 50612→8080 [ACK] Seq=531 Ack=62949 Win=525568 Len=0
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       TCP      1514 [TCP segment of a reassembled PDU]
.168.0.3       HTTP      234 HTTP/1.1 206 Partial Content  (application/octet-stream)
.168.255.13    TCP        54 50612→8080 [ACK] Seq=531 Ack=66049 Win=525568 Len=0
.168.0.3       TPKT       93 Continuation
```

```
⊞ Fr  101 bytes captured (808 bits) on interface 0
⊞ Et  0:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Ir  168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Tr  t: 3389 (3389), Dst Port: 4459 (4459), Seq: 1, Ack: 1, Len: 47
⊞ TF
```

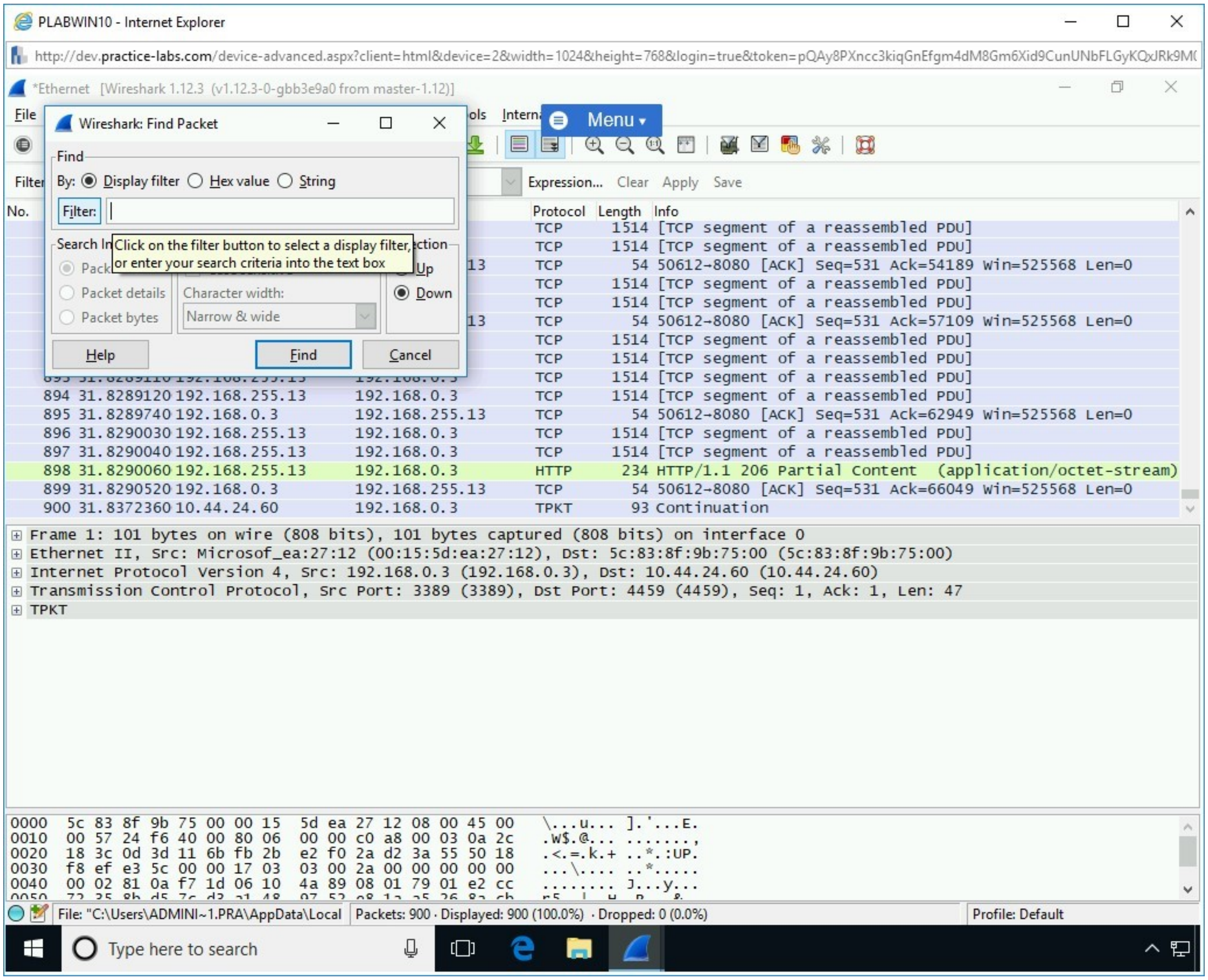
```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 24 f6 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .W$.@... .......,
0020  18 3c 0d 3d 11 6b fb 2b  e2 f0 2a d2 3a 55 50 18   .<.=.k.+ ..*.:UP.
0030  f8 ef e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 02 81 0a f7 1d 06 10  4a 89 08 01 79 01 e2 cc   ........ J...y...
```

File: "C:\Users\ADMINI~1.PRA\AppData\Local Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%)

Figure 1.72 Screenshot of PLABWIN10: Selecting Find Packet from the Edit menu.

Step 6

The **Wireshark: Find Packet** dialog box is displayed. Click **Filter**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File
Menu ▾
Expression... Clear Apply Save
Type here to search

Wireshark: Find Packet

Find

By: ● Display filter ○ Hex value ○ String

Filter: |

Click on the filter button to select a display filter, or enter your search criteria into the text box

Search In: ○ Packet list ○ Packet details ○ Packet bytes

Character width: Narrow & wide

Direction: ○ Up ● Down

Help | Find | Cancel

```
No.                                                  Protocol Length Info
                                                     TCP      1514 [TCP segment of a reassembled PDU]
                                                     TCP      1514 [TCP segment of a reassembled PDU]
                                                  13 TCP        54 50612→8080 [ACK] Seq=531 Ack=54189 Win=525568 Len=0
                                                     TCP      1514 [TCP segment of a reassembled PDU]
                                                     TCP      1514 [TCP segment of a reassembled PDU]
                                                  13 TCP        54 50612→8080 [ACK] Seq=531 Ack=57109 Win=525568 Len=0
                                                     TCP      1514 [TCP segment of a reassembled PDU]
                                                     TCP      1514 [TCP segment of a reassembled PDU]
                                                     TCP      1514 [TCP segment of a reassembled PDU]
894 31.8289120 192.168.255.13   192.168.0.3          TCP      1514 [TCP segment of a reassembled PDU]
895 31.8289740 192.168.0.3      192.168.255.13       TCP        54 50612→8080 [ACK] Seq=531 Ack=62949 Win=525568 Len=0
896 31.8290030 192.168.255.13   192.168.0.3          TCP      1514 [TCP segment of a reassembled PDU]
897 31.8290040 192.168.255.13   192.168.0.3          TCP      1514 [TCP segment of a reassembled PDU]
898 31.8290060 192.168.255.13   192.168.0.3          HTTP      234 HTTP/1.1 206 Partial Content  (application/octet-stream)
899 31.8290520 192.168.0.3      192.168.255.13       TCP        54 50612→8080 [ACK] Seq=531 Ack=66049 Win=525568 Len=0
900 31.8372360 10.44.24.60      192.168.0.3          TPKT       93 Continuation
```

```
⊞ Frame 1: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 4459 (4459), Seq: 1, Ack: 1, Len: 47
⊞ TPKT
```

```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 24 f6 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .W$.@... .......,
0020  18 3c 0d 3d 11 6b fb 2b  e2 f0 2a d2 3a 55 50 18   .<.=.k.+ ..*.:UP.
0030  f8 ef e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 02 81 0a f7 1d 06 10  4a 89 08 01 79 01 e2 cc   ........ J...y...
```

File: "C:\Users\ADMINI~1.PRA\AppData\Local | Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

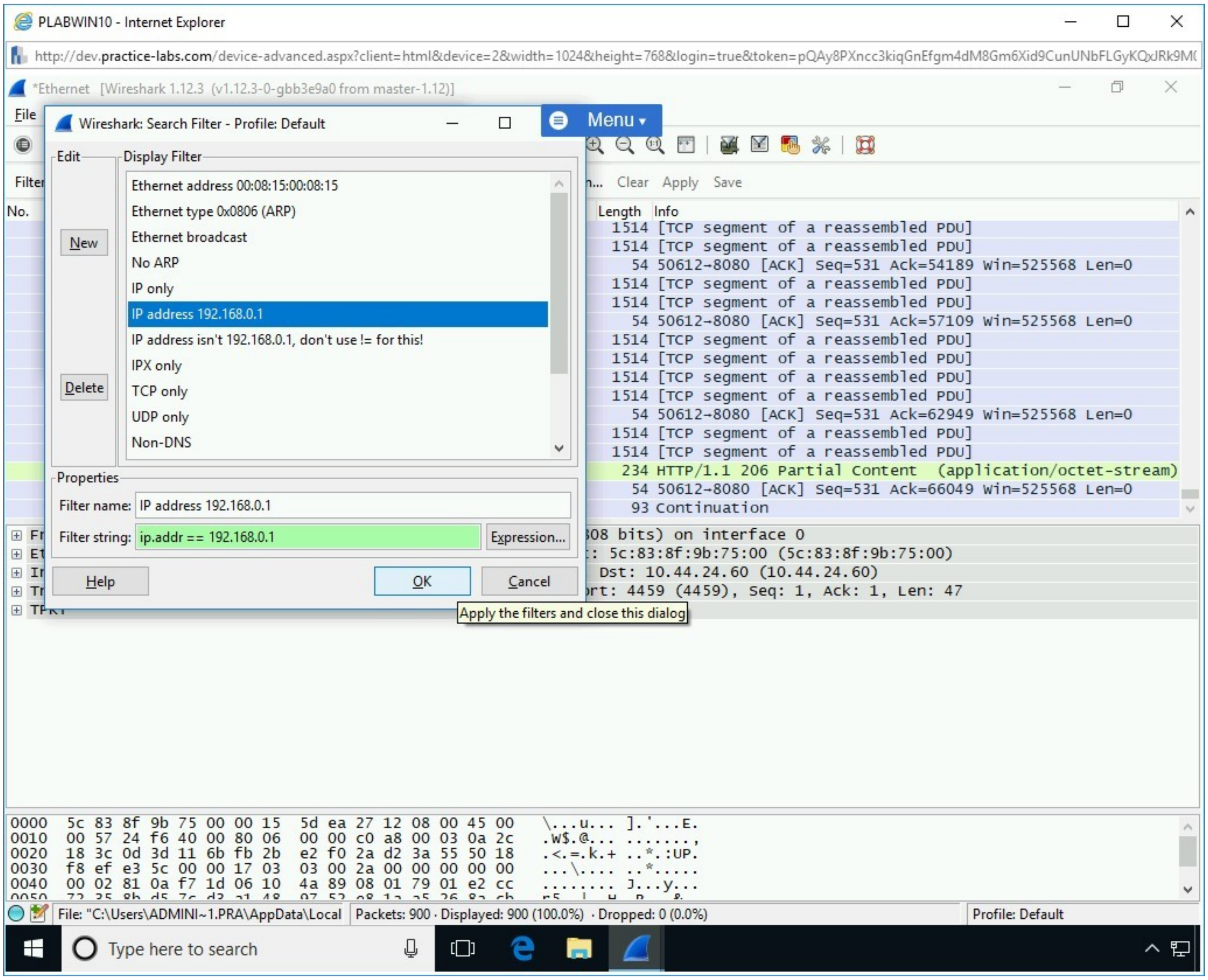
Figure 1.73 Screenshot of PLABWIN10: Clicking Filter on the Wireshark: Find Packet dialog box.

Step 7

The **Wireshark: Search Filter** dialog box is displayed.

You have the option to filter the results. Select **IP address 192.168.0.1**.

Click **OK**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
Wireshark: Search Filter - Profile: Default
Menu
Edit
New
Delete
Display Filter
Properties
Expression...
Help
OK
Cancel
Apply the filters and close this dialog
Clear
Apply
Save
Type here to search
Profile: Default

Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
Non-DNS

Filter name: IP address 192.168.0.1

Filter string: ip.addr == 192.168.0.1

```
Length  Info
  1514 [TCP segment of a reassembled PDU]
  1514 [TCP segment of a reassembled PDU]
    54 50612→8080 [ACK] Seq=531 Ack=54189 Win=525568 Len=0
  1514 [TCP segment of a reassembled PDU]
  1514 [TCP segment of a reassembled PDU]
    54 50612→8080 [ACK] Seq=531 Ack=57109 Win=525568 Len=0
  1514 [TCP segment of a reassembled PDU]
  1514 [TCP segment of a reassembled PDU]
  1514 [TCP segment of a reassembled PDU]
  1514 [TCP segment of a reassembled PDU]
    54 50612→8080 [ACK] Seq=531 Ack=62949 Win=525568 Len=0
  1514 [TCP segment of a reassembled PDU]
  1514 [TCP segment of a reassembled PDU]
   234 HTTP/1.1 206 Partial Content  (application/octet-stream)
    54 50612→8080 [ACK] Seq=531 Ack=66049 Win=525568 Len=0
    93 Continuation
```

```
308 bits) on interface 0
: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
 Dst: 10.44.24.60 (10.44.24.60)
rt: 4459 (4459), Seq: 1, Ack: 1, Len: 47
```

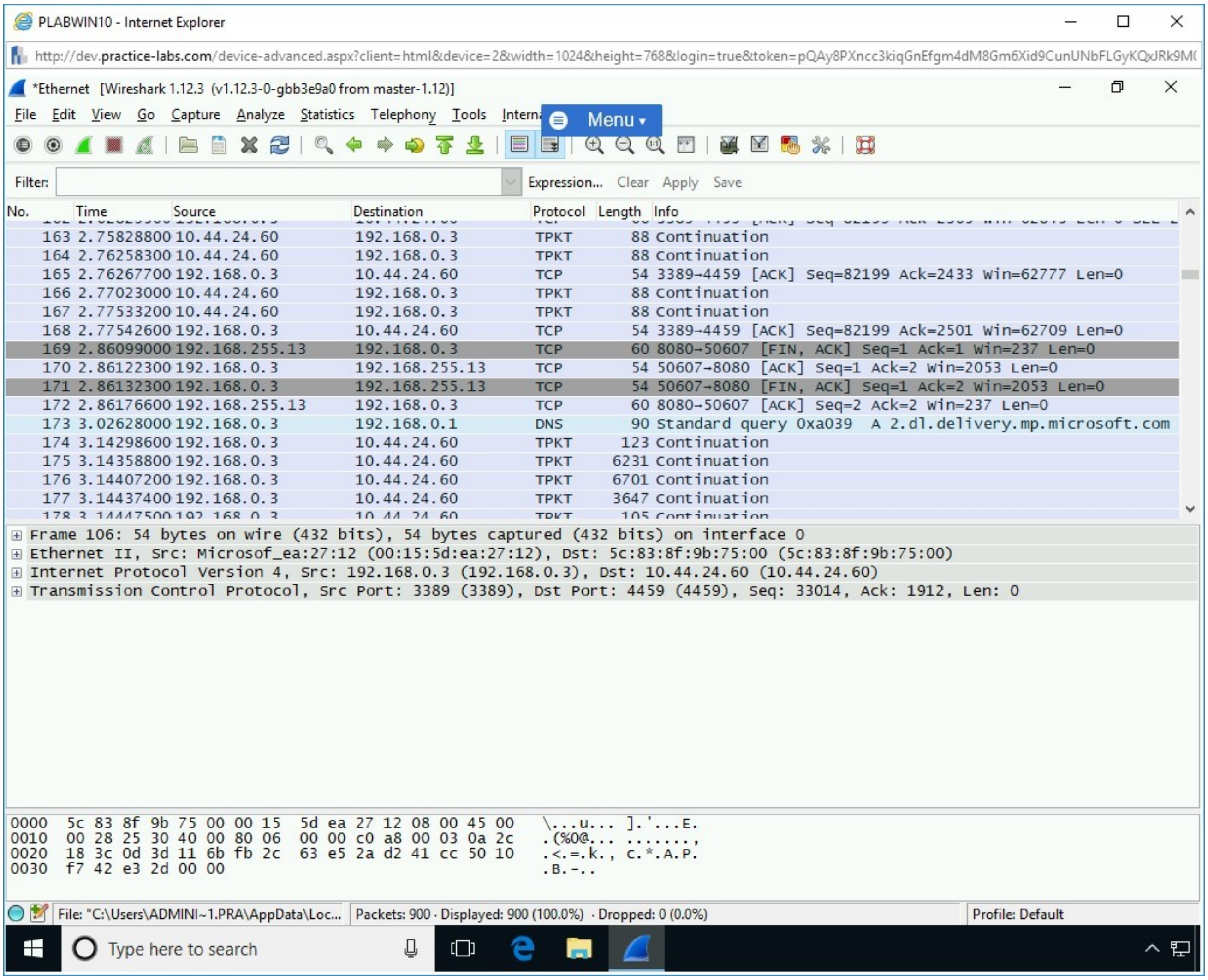
```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 57 24 f6 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .W$.@... .......,
0020  18 3c 0d 3d 11 6b fb 2b  e2 f0 2a d2 3a 55 50 18   .<.=.k.+ ..*.:UP.
0030  f8 ef e3 5c 00 00 17 03  03 00 2a 00 00 00 00 00   ...\.... ..*.....
0040  00 02 81 0a f7 1d 06 10  4a 89 08 01 79 01 e2 cc   ........ J...y...
```

File: "C:\Users\ADMINI~1.PRA\AppData\Local   Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%)

Figure 1.74 Screenshot of PLABWIN10: Selecting IP address 192.168.0.1 and clicking OK.

Step 8

Scroll down the list. Note that the results are now highlighted in a light blue color.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Interna
Menu ▾
Filter:
Expression... Clear Apply Save
Type here to search

```
No.   Time        Source          Destination     Protocol Length Info
  163 2.75828800 10.44.24.60     192.168.0.3     TPKT       88 Continuation
  164 2.76258300 10.44.24.60     192.168.0.3     TPKT       88 Continuation
  165 2.76267700 192.168.0.3     10.44.24.60     TCP        54 3389→4459 [ACK] Seq=82199 Ack=2433 Win=62777 Len=0
  166 2.77023000 10.44.24.60     192.168.0.3     TPKT       88 Continuation
  167 2.77533200 10.44.24.60     192.168.0.3     TPKT       88 Continuation
  168 2.77542600 192.168.0.3     10.44.24.60     TCP        54 3389→4459 [ACK] Seq=82199 Ack=2501 Win=62709 Len=0
  169 2.86099000 192.168.255.13  192.168.0.3     TCP        60 8080→50607 [FIN, ACK] Seq=1 Ack=1 Win=237 Len=0
  170 2.86122300 192.168.0.3     192.168.255.13  TCP        54 50607→8080 [ACK] Seq=1 Ack=2 Win=2053 Len=0
  171 2.86132300 192.168.0.3     192.168.255.13  TCP        54 50607→8080 [FIN, ACK] Seq=1 Ack=2 Win=2053 Len=0
  172 2.86176600 192.168.255.13  192.168.0.3     TCP        60 8080→50607 [ACK] Seq=2 Ack=2 Win=237 Len=0
  173 3.02628000 192.168.0.3     192.168.0.1     DNS        90 Standard query 0xa039  A 2.dl.delivery.mp.microsoft.com
  174 3.14298600 192.168.0.3     10.44.24.60     TPKT      123 Continuation
  175 3.14358800 192.168.0.3     10.44.24.60     TPKT     6231 Continuation
  176 3.14407200 192.168.0.3     10.44.24.60     TPKT     6701 Continuation
  177 3.14437400 192.168.0.3     10.44.24.60     TPKT     3647 Continuation
  178 3.14447500 192.168.0.3     10.44.24.60     TPKT      105 Continuation
```

```
⊞ Frame 106: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 4459 (4459), Seq: 33014, Ack: 1912, Len: 0
```

```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 28 25 30 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .(%0@... .......,
0020  18 3c 0d 3d 11 6b fb 2c  63 e5 2a d2 41 cc 50 10   .<.=.k., c.*.A.P.
0030  f7 42 e3 2d 00 00                                  .B.-..
```

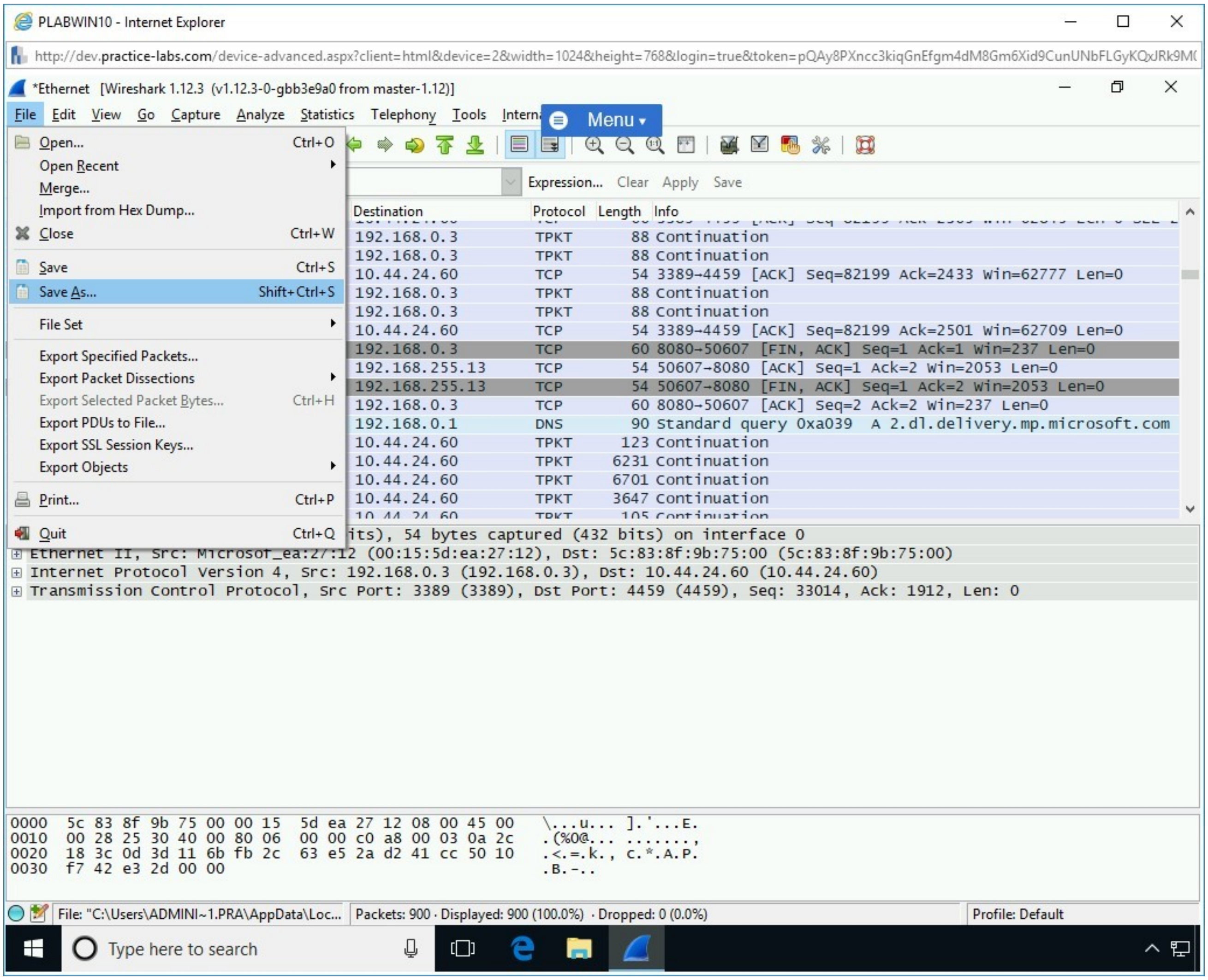
File: "C:\Users\ADMINI~1.PRA\AppData\Loc... | Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Figure 1.75 Screenshot of PLABWIN10: Showing the result of the selected filter in Wireshark.

Step 9

Now, you will save the results in a log file.

Click **File** and select **Save As.**


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(
*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Intern
Menu ▾
Open... Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Shift+Ctrl+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Selected Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Expression... Clear Apply Save
Type here to search

```
Destination      Protocol  Length Info
192.168.0.3      TPKT        88 Continuation
192.168.0.3      TPKT        88 Continuation
10.44.24.60      TCP         54 3389→4459 [ACK] Seq=82199 Ack=2433 Win=62777 Len=0
192.168.0.3      TPKT        88 Continuation
192.168.0.3      TPKT        88 Continuation
10.44.24.60      TCP         54 3389→4459 [ACK] Seq=82199 Ack=2501 Win=62709 Len=0
192.168.0.3      TCP         60 8080→50607 [FIN, ACK] Seq=1 Ack=1 Win=237 Len=0
192.168.255.13   TCP         54 50607→8080 [ACK] Seq=1 Ack=2 Win=2053 Len=0
192.168.255.13   TCP         54 50607→8080 [FIN, ACK] Seq=1 Ack=2 Win=2053 Len=0
192.168.0.3      TCP         60 8080→50607 [ACK] Seq=2 Ack=2 Win=237 Len=0
192.168.0.1      DNS         90 Standard query 0xa039  A 2.dl.delivery.mp.microsoft.com
10.44.24.60      TPKT       123 Continuation
10.44.24.60      TPKT      6231 Continuation
10.44.24.60      TPKT      6701 Continuation
10.44.24.60      TPKT      3647 Continuation
```

```
its), 54 bytes captured (432 bits) on interface 0
⊞ Ethernet II, Src: Microsof_ea:27:12 (00:15:5d:ea:27:12), Dst: 5c:83:8f:9b:75:00 (5c:83:8f:9b:75:00)
⊞ Internet Protocol Version 4, Src: 192.168.0.3 (192.168.0.3), Dst: 10.44.24.60 (10.44.24.60)
⊞ Transmission Control Protocol, Src Port: 3389 (3389), Dst Port: 4459 (4459), Seq: 33014, Ack: 1912, Len: 0
```

```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 28 25 30 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .(%0@... .......,
0020  18 3c 0d 3d 11 6b fb 2c  63 e5 2a d2 41 cc 50 10   .<.=.k., c.*.A.P.
0030  f7 42 e3 2d 00 00                                  .B.-..
```

File: "C:\Users\ADMINI~1.PRA\AppData\Loc... | Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

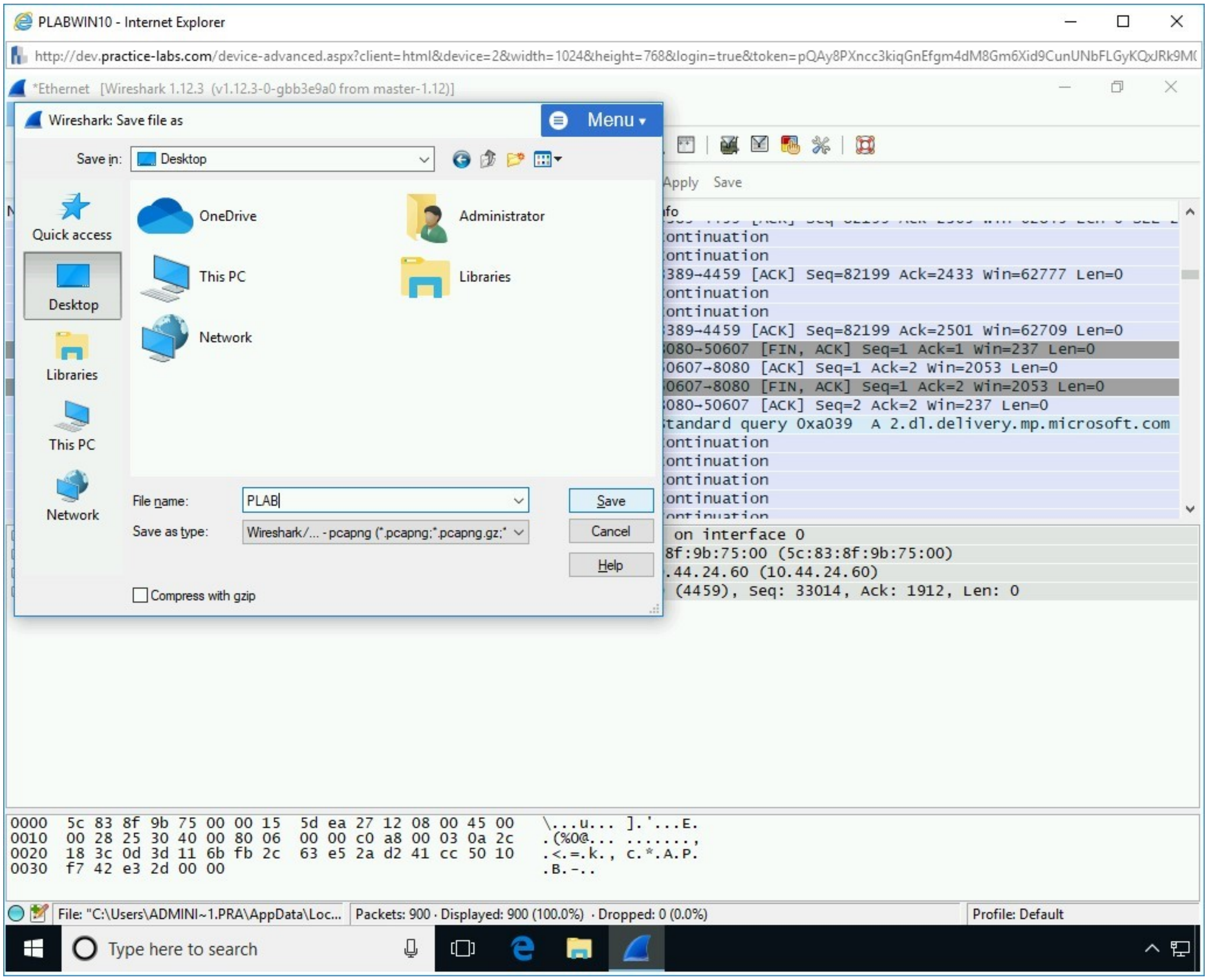
Figure 1.76 Screenshot of PLABWIN10: Selecting Save As in the File menu.

Step 10

The **Wireshark: Save file as** dialog box is displayed.

Enter file name: **PLAB**

Select **Desktop** from the left-hand pane and then click **Save**.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M(

*Ethernet [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Wireshark: Save file as

Save in: Desktop

File name: PLAB

Save as type: Wireshark/... - pcapng (*.pcapng;*.pcapng.gz;*

□ Compress with gzip

```
ontinuation
ontinuation
389→4459 [ACK] Seq=82199 Ack=2433 Win=62777 Len=0
ontinuation
ontinuation
389→4459 [ACK] Seq=82199 Ack=2501 Win=62709 Len=0
080→50607 [FIN, ACK] Seq=1 Ack=1 Win=237 Len=0
0607→8080 [ACK] Seq=1 Ack=2 Win=2053 Len=0
0607→8080 [FIN, ACK] Seq=1 Ack=2 Win=2053 Len=0
080→50607 [ACK] Seq=2 Ack=2 Win=237 Len=0
tandard query 0xa039  A 2.dl.delivery.mp.microsoft.com
ontinuation
ontinuation
ontinuation
ontinuation
```

```
 on interface 0
8f:9b:75:00 (5c:83:8f:9b:75:00)
.44.24.60 (10.44.24.60)
 (4459), Seq: 33014, Ack: 1912, Len: 0
```

```
0000  5c 83 8f 9b 75 00 00 15  5d ea 27 12 08 00 45 00   \...u... ].'...E.
0010  00 28 25 30 40 00 80 06  00 00 c0 a8 00 03 0a 2c   .(%0@... .......,
0020  18 3c 0d 3d 11 6b fb 2c  63 e5 2a d2 41 cc 50 10   .<.=.k., c.*.A.P.
0030  f7 42 e3 2d 00 00                                  .B.-..
```

File: "C:\Users\ADMINI~1.PRA\AppData\Loc... | Packets: 900 · Displayed: 900 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Figure 1.77 Screenshot of PLABWIN10: Naming the file as PLAB to save on the Desktop. Clicking save.

Step 11

Close **WireShark**. You are now on the desktop. Notice that the saved log file with the name **PLAB** is now available.

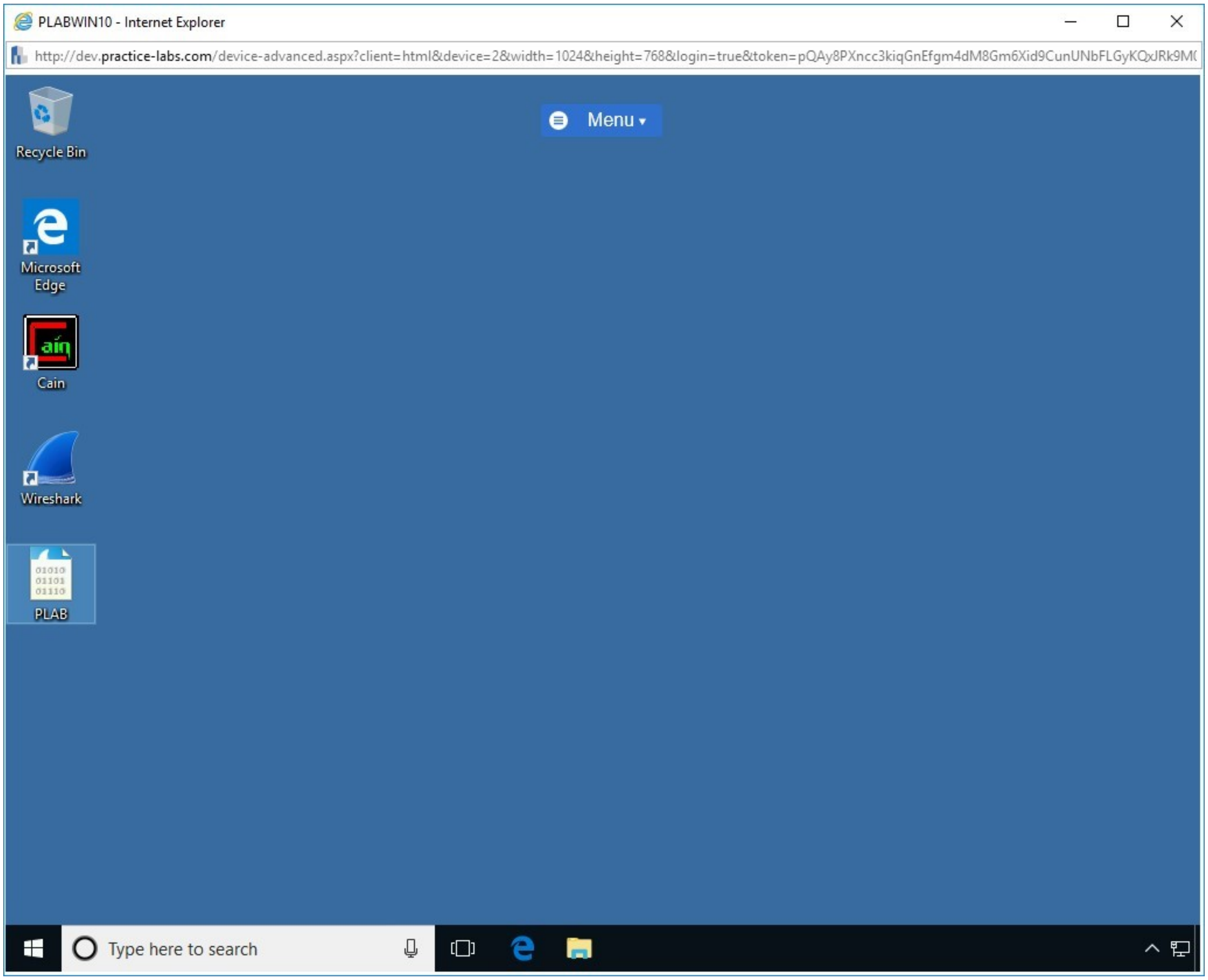

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=pQAy8PXncc3kiqGnEfgm4dM8Gm6Xid9CunUNbFLGyKQxJRk9M
Menu
Recycle Bin
Microsoft Edge
Cain
Wireshark
PLAB
Type here to search

Figure 1.78 Screenshot of PLABWIN10: Showing the packet capture file on the desktop.

Task 5 - Use Sniff-O-Matic

Sniff-O-Matic is a tool that not only works as a packet sniffer but also as a network protocol analyzer. It can capture packets from the network and present packet information in a particular structure to ensure ease of analysis.

In this task, you will learn to use **Sniff-O-Matic**.

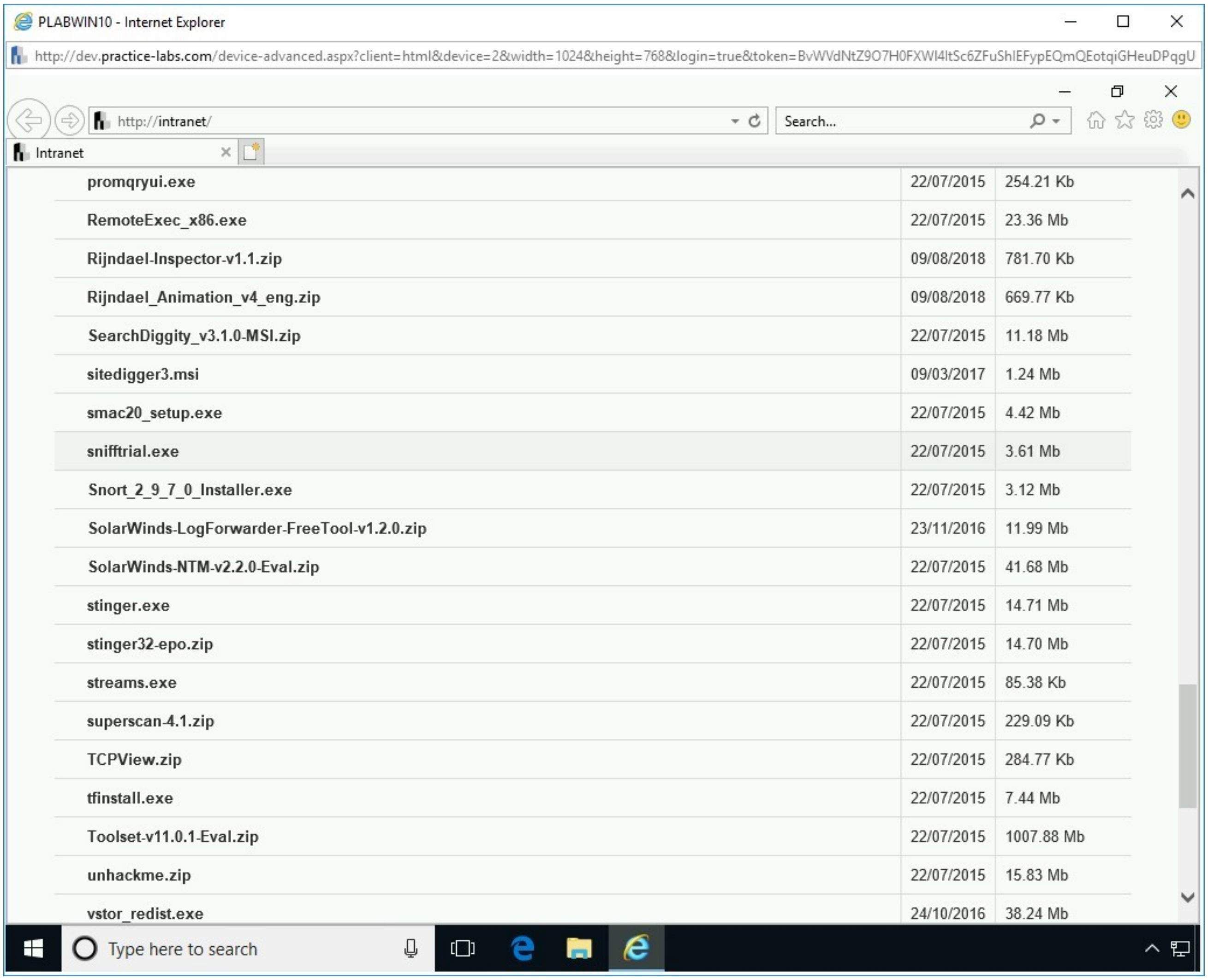
To use **Sniff-O-Matic**, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**.

Re-open **Internet Explorer**, and navigate back to the **Tools** > **Hacking Tools** page of the intranet.

Locate **snifftrial.exe**, and then click on it.



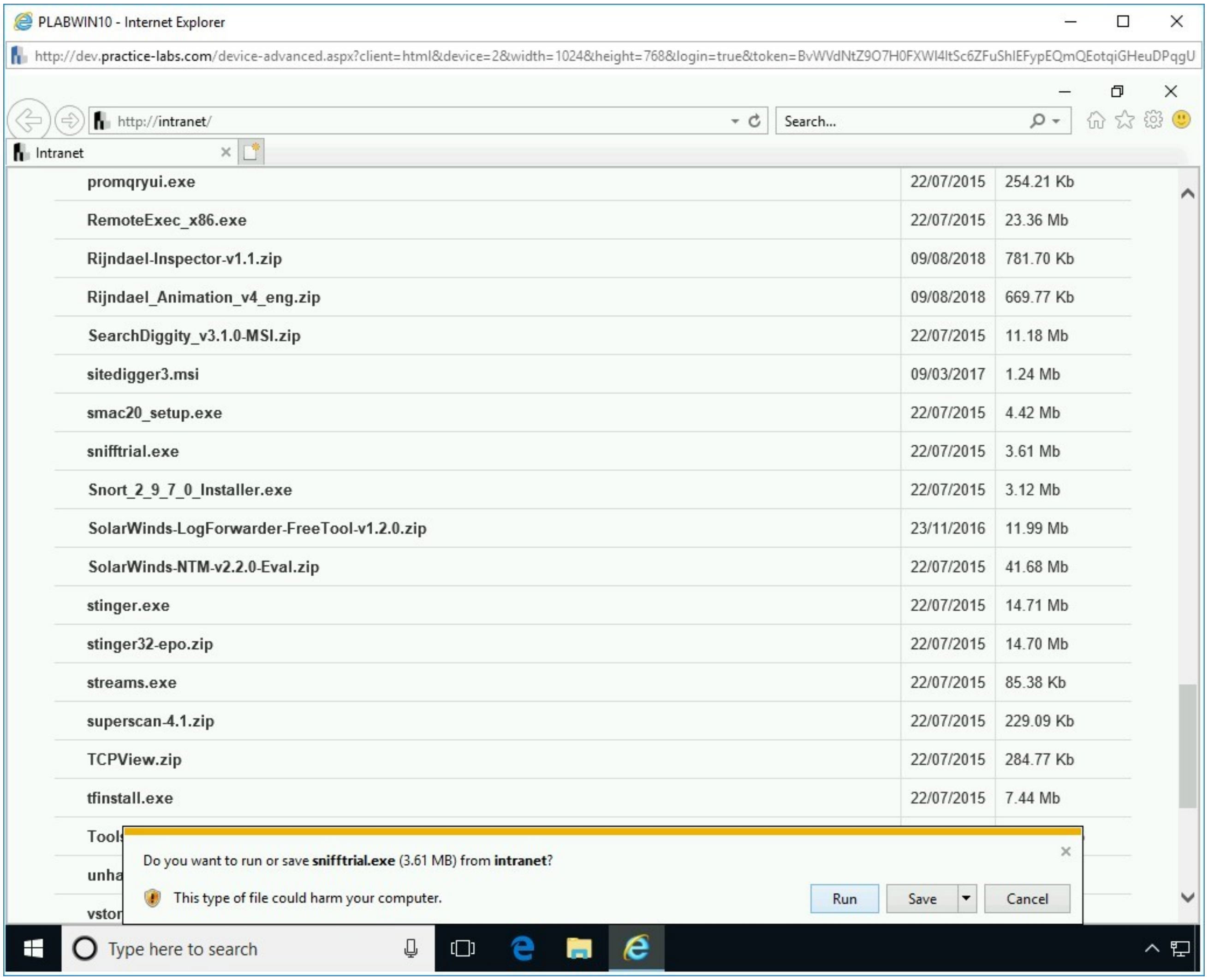
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Type here to search

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Figure 1.79 Screenshot of PLABWIN10: Intranet window displayed. Clicking the snifftrail.exe file.

Step 2

In the notification bar, click **Run**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Run
Save
Cancel
Type here to search

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zip	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-FreeTool-v1.2.0.zip	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zip	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Tool		
unha		
vstor		

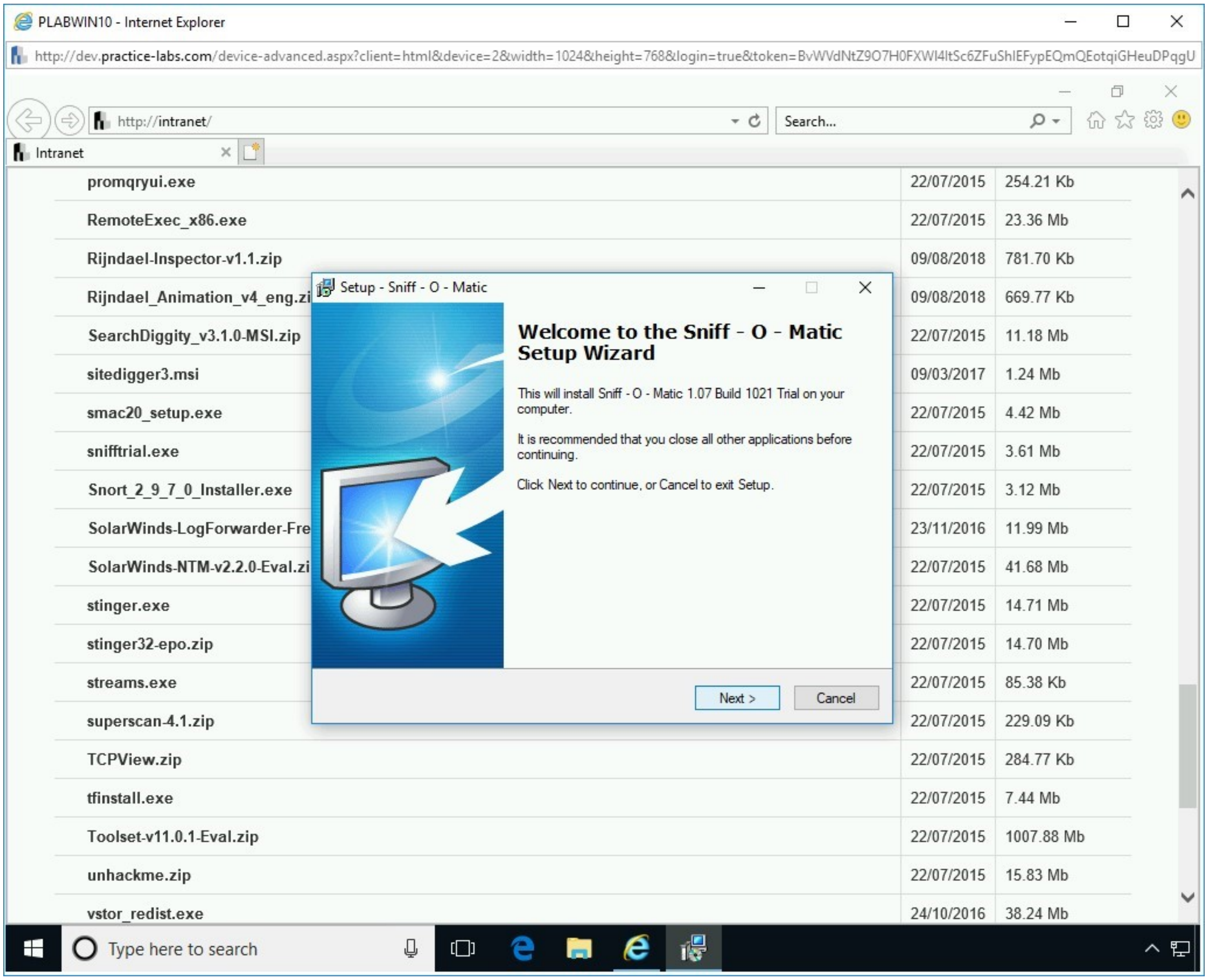
Do you want to run or save **snifftrial.exe** (3.61 MB) from **intranet**?

This type of file could harm your computer.

Figure 1.80 Screenshot of PLABWIN10: Clicking Run on the notification bar.

Step 3

The **Setup - Sniff - O - Matic** wizard is displayed. On the **Welcome to the Sniff - O - Matic Setup Wizard** page, click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Type here to search

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

Welcome to the Sniff - O - Matic Setup Wizard

This will install Sniff - O - Matic 1.07 Build 1021 Trial on your computer.

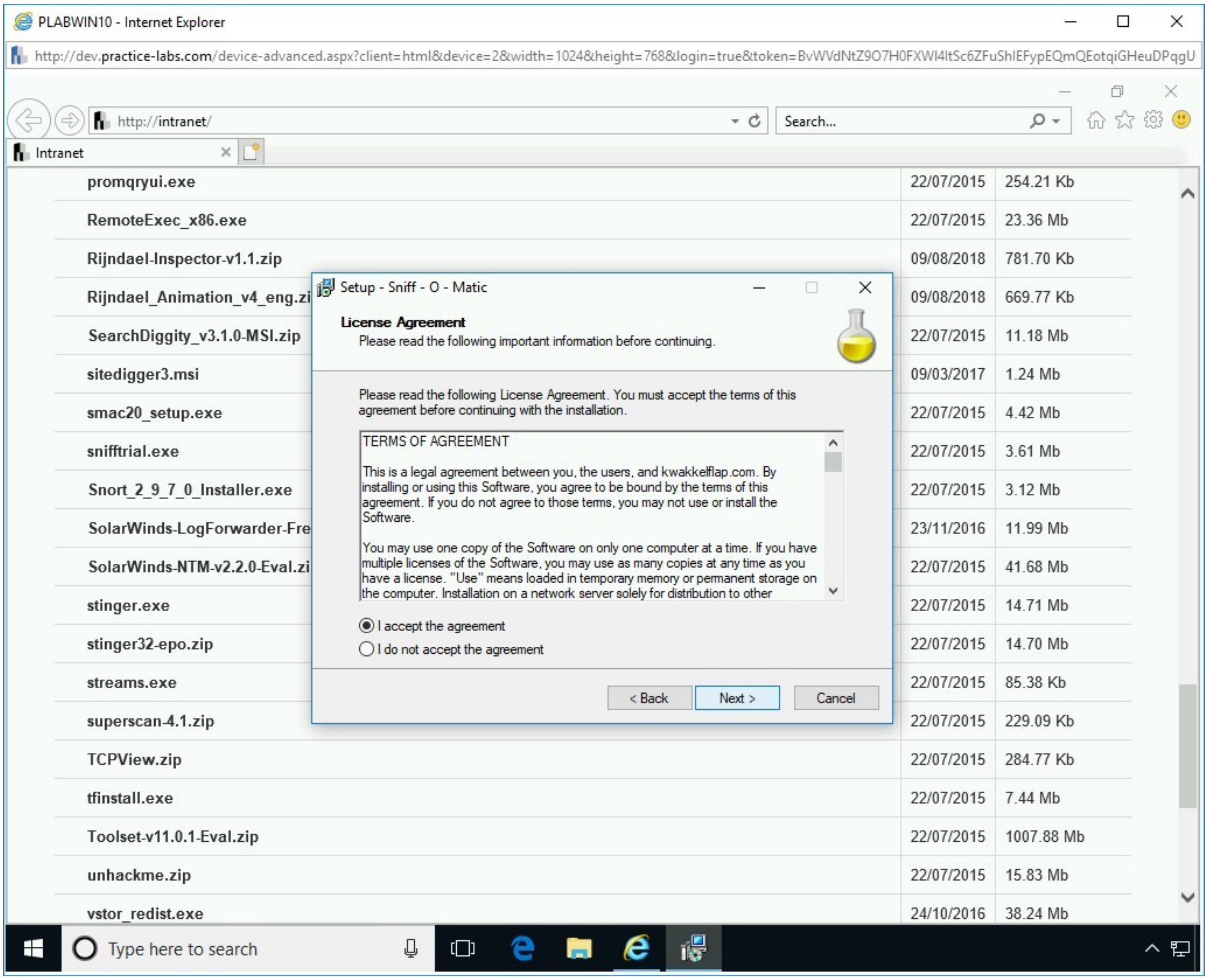
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 1.81 Screenshot of PLABWIN10: Clicking Next on the welcome page.

Step 4

On the **License Agreement** page, select **I accept the agreement** and click **Next**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

TERMS OF AGREEMENT

This is a legal agreement between you, the users, and kwakkelflap.com. By installing or using this Software, you agree to be bound by the terms of this agreement. If you do not agree to those terms, you may not use or install the Software.

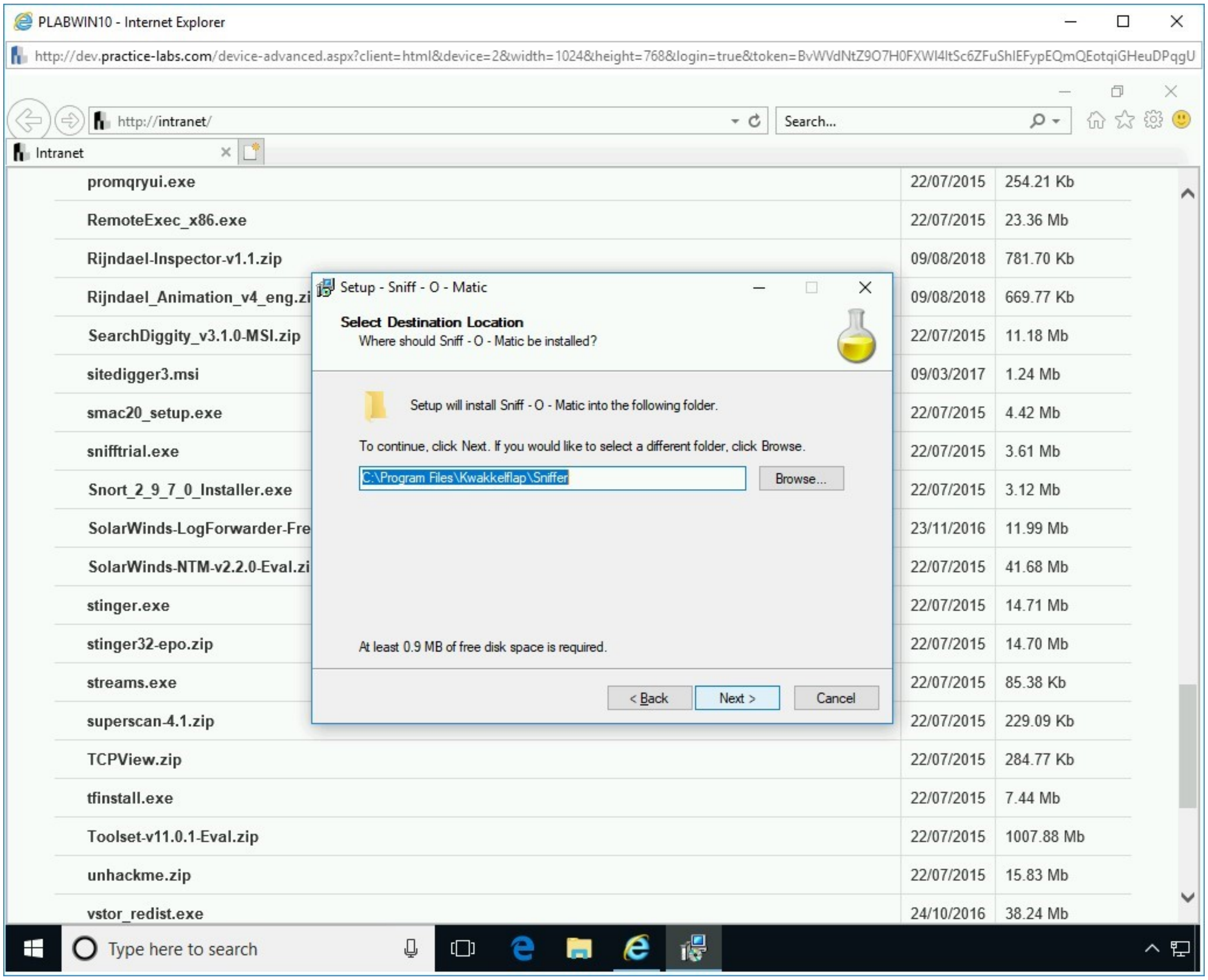
You may use one copy of the Software on only one computer at a time. If you have multiple licenses of the Software, you may use as many copies at any time as you have a license. "Use" means loaded in temporary memory or permanent storage on the computer. Installation on a network server solely for distribution to other

● I accept the agreement
○ I do not accept the agreement

Figure 1.82 Screenshot of PLABWIN10: Clicking I accept the agreement on the License Agreement page and clicking Next.

Step 5

On the **Select Destination Location** page, keep the default path, and click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Type here to search
< Back
Next >
Cancel
Browse...

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

Select Destination Location

Where should Sniff - O - Matic be installed?

Setup will install Sniff - O - Matic into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

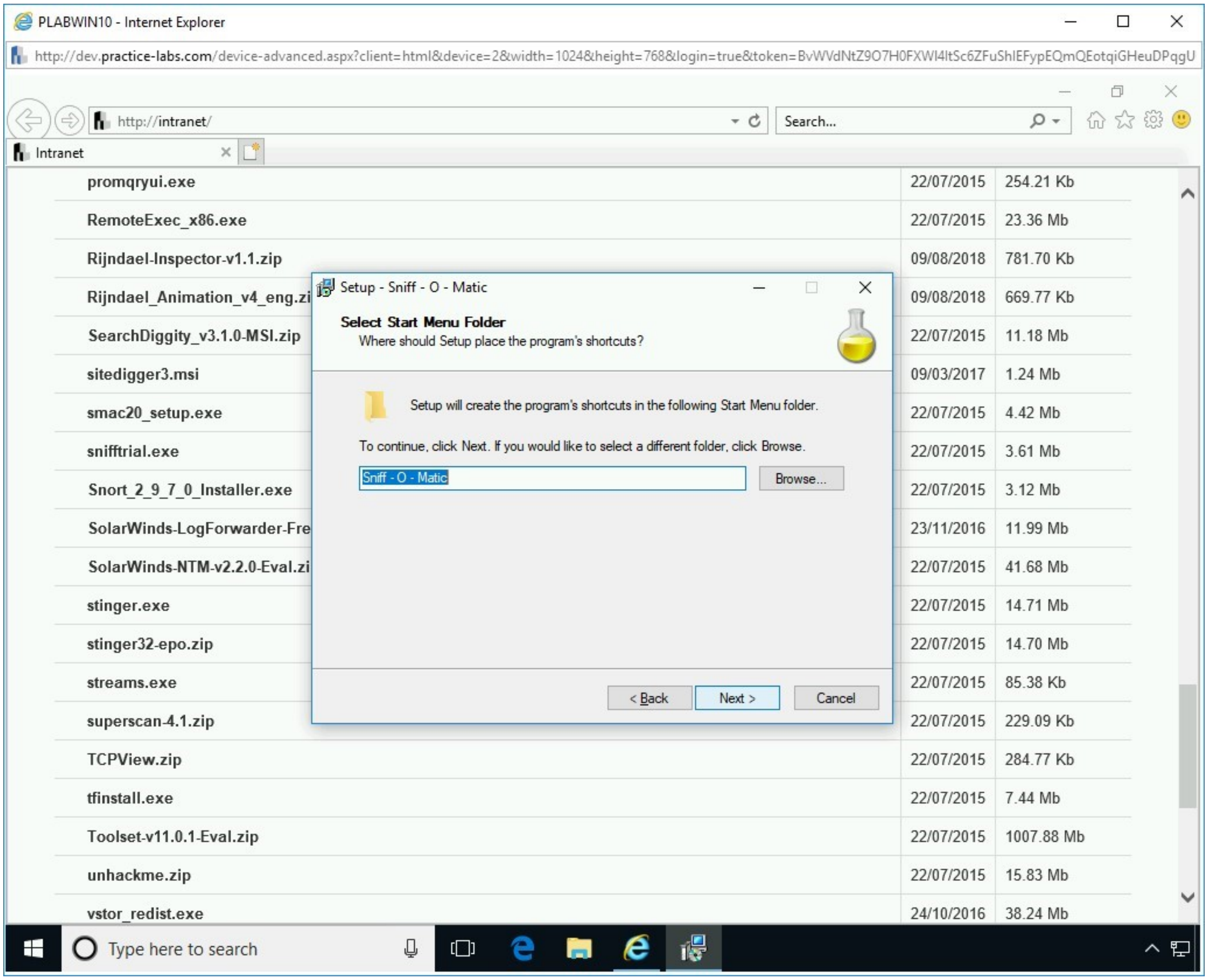
C:\Program Files\Kwakkelflap\Sniffer

At least 0.9 MB of free disk space is required.

Figure 1.83 Screenshot of PLABWIN10: Selecting the default installation path and clicking Next.

Step 6

On the **Select Start Menu Folder** page, keep the default menu name, click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Type here to search

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

Select Start Menu Folder

Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

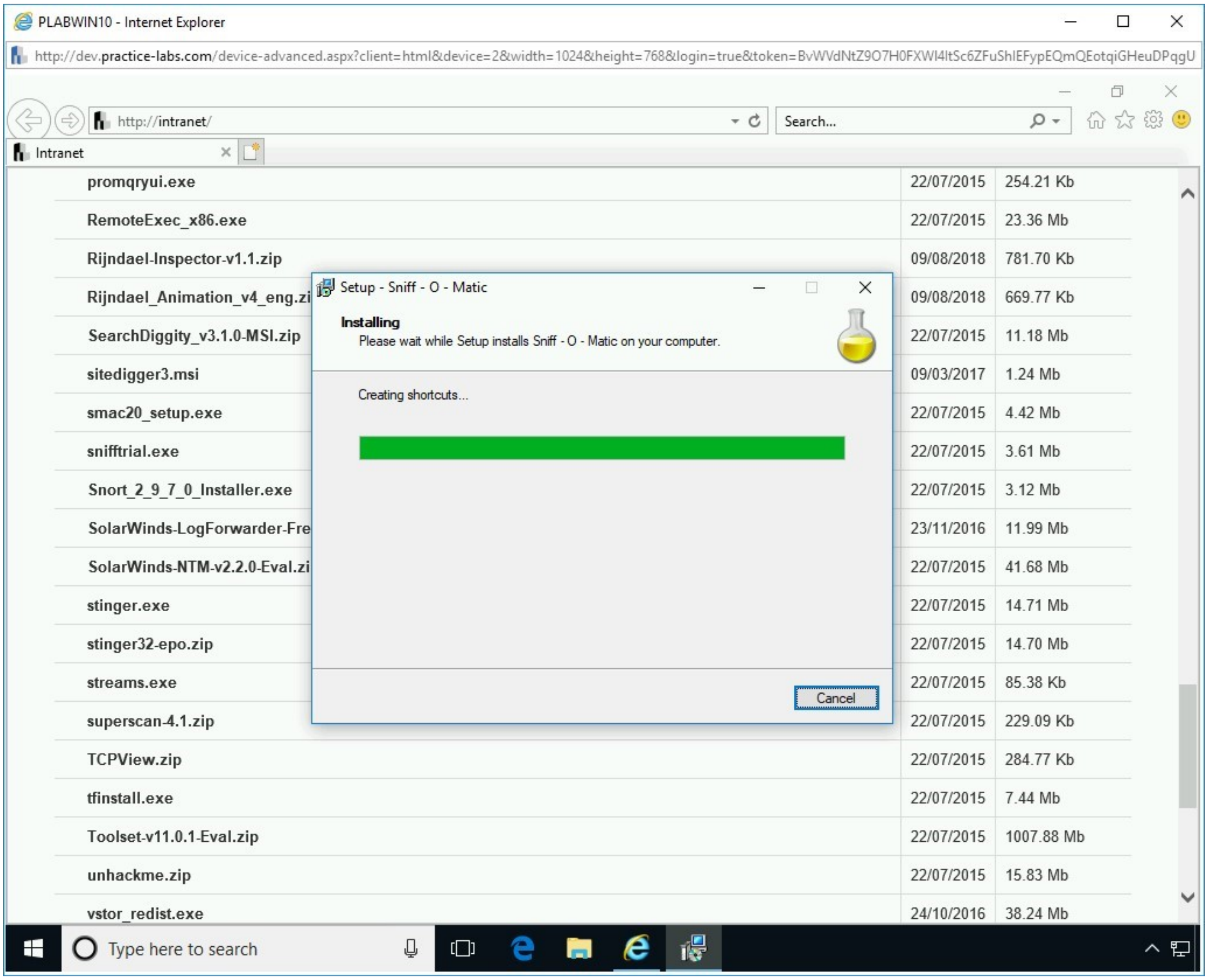
Sniff - O - Matic

Figure 1.84 Screenshot of PLABWIN10: Keeping the default menu folder and clicking Next.

Step 7

On the **Ready to Install** page, review the configuration, and click **Install**.

The installation process starts.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShIEFypEQmQEotqiGHeuDPqgU

http://intranet/

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

Installing

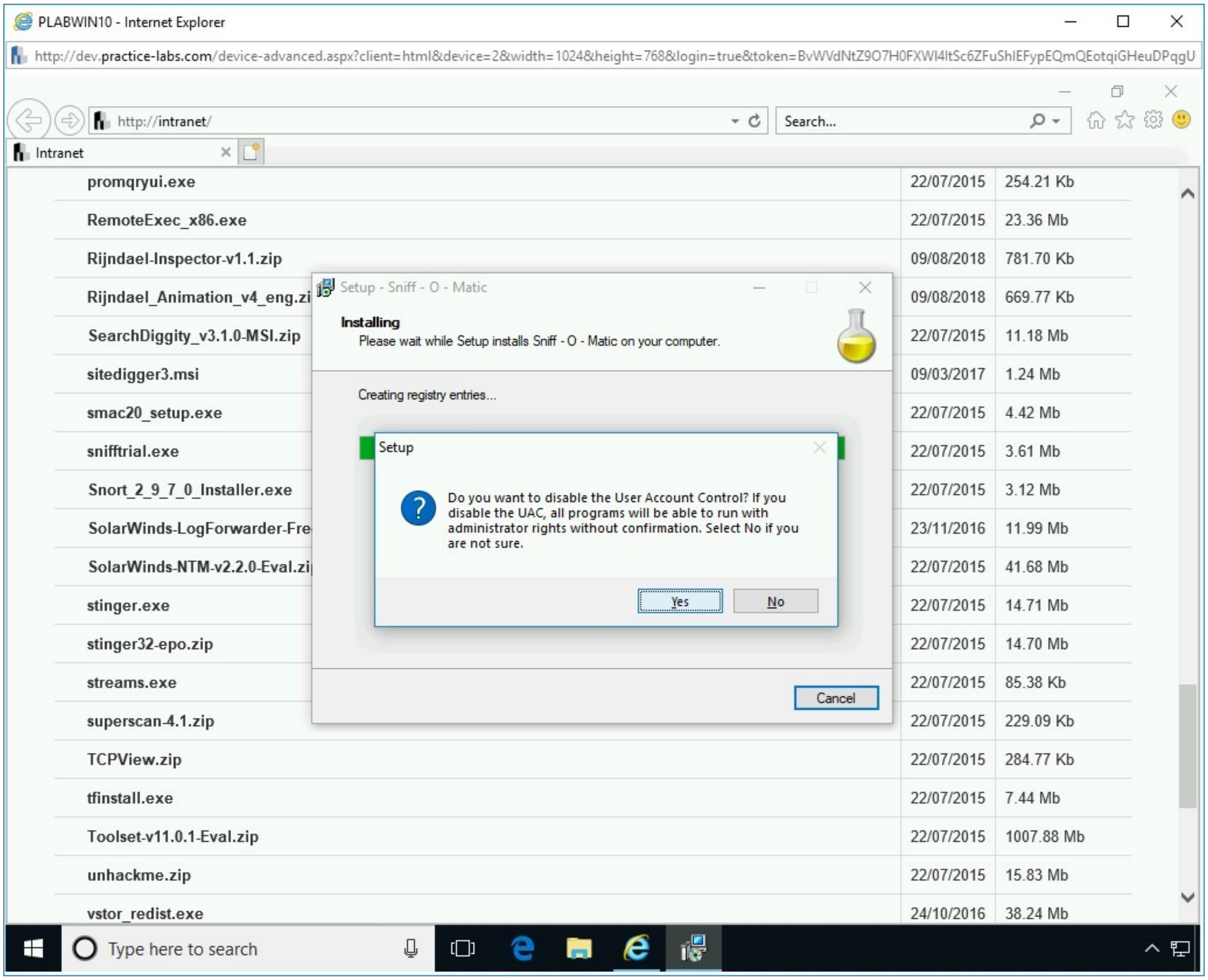
Please wait while Setup installs Sniff - O - Matic on your computer.

Creating shortcuts...

Figure 1.85 Screenshot of PLABWIN10: Showing the installation progress on the Installing page.

Step 8

At the end of the installation, you will be asked if you want to disable the **User Account Control**, click **Yes.**



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU

http://intranet/

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

Installing

Please wait while Setup installs Sniff - O - Matic on your computer.

Creating registry entries...

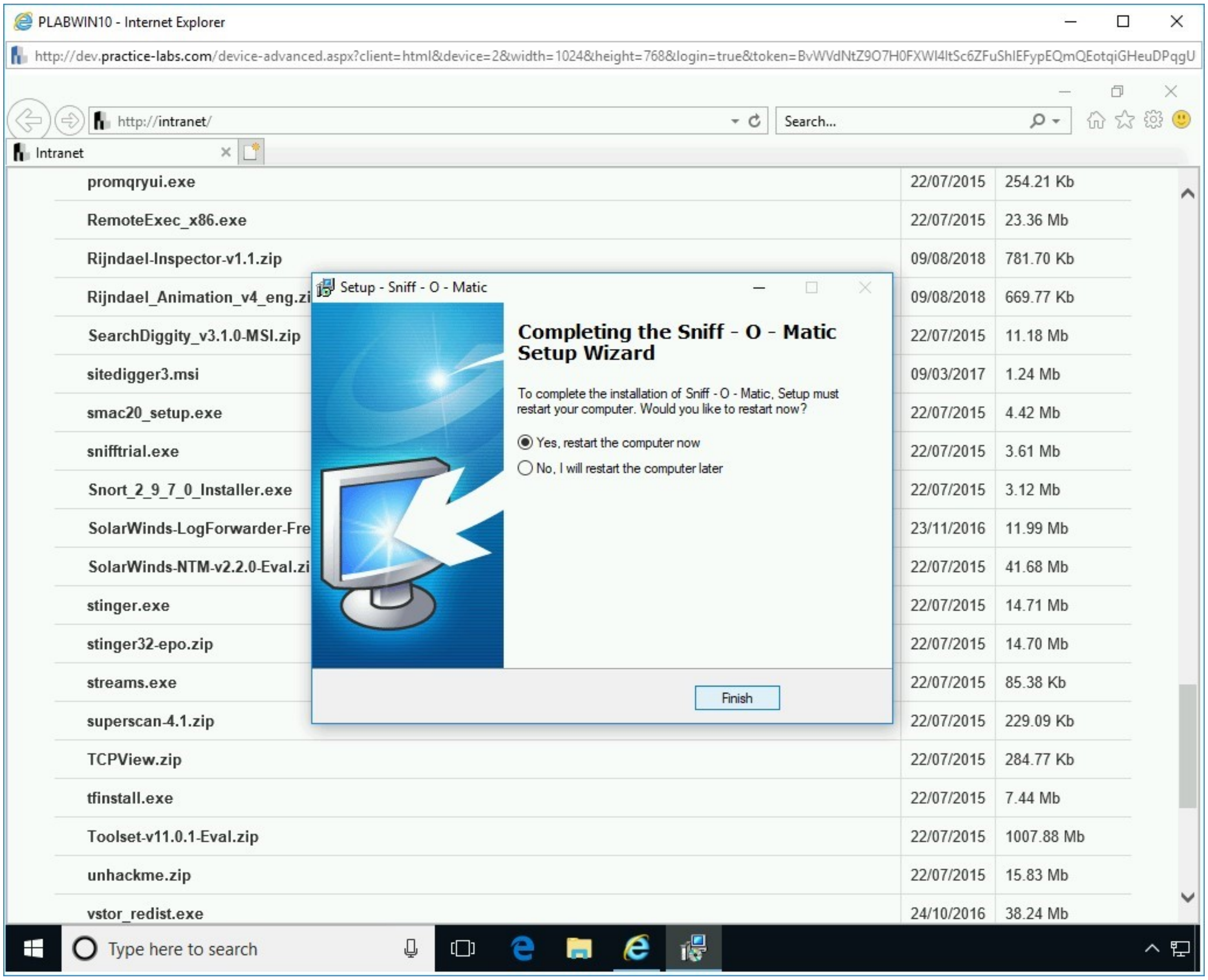
Setup

Do you want to disable the User Account Control? If you disable the UAC, all programs will be able to run with administrator rights without confirmation. Select No if you are not sure.

Figure 1.86 Screenshot of PLABWIN10: Clicking Yes on the Setup dialog box.

Step 9

On the **Completing the Sniff - O - Matic Setup Wizard** page, keep the default selection and click **Finish**. This will restart **PLABWIN10**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Type here to search

promqryui.exe	22/07/2015	254.21 Kb
RemoteExec_x86.exe	22/07/2015	23.36 Mb
Rijndael-Inspector-v1.1.zip	09/08/2018	781.70 Kb
Rijndael_Animation_v4_eng.zi	09/08/2018	669.77 Kb
SearchDiggity_v3.1.0-MSI.zip	22/07/2015	11.18 Mb
sitedigger3.msi	09/03/2017	1.24 Mb
smac20_setup.exe	22/07/2015	4.42 Mb
snifftrial.exe	22/07/2015	3.61 Mb
Snort_2_9_7_0_Installer.exe	22/07/2015	3.12 Mb
SolarWinds-LogForwarder-Fre	23/11/2016	11.99 Mb
SolarWinds-NTM-v2.2.0-Eval.zi	22/07/2015	41.68 Mb
stinger.exe	22/07/2015	14.71 Mb
stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb

Setup - Sniff - O - Matic

Completing the Sniff - O - Matic Setup Wizard

To complete the installation of Sniff - O - Matic, Setup must restart your computer. Would you like to restart now?

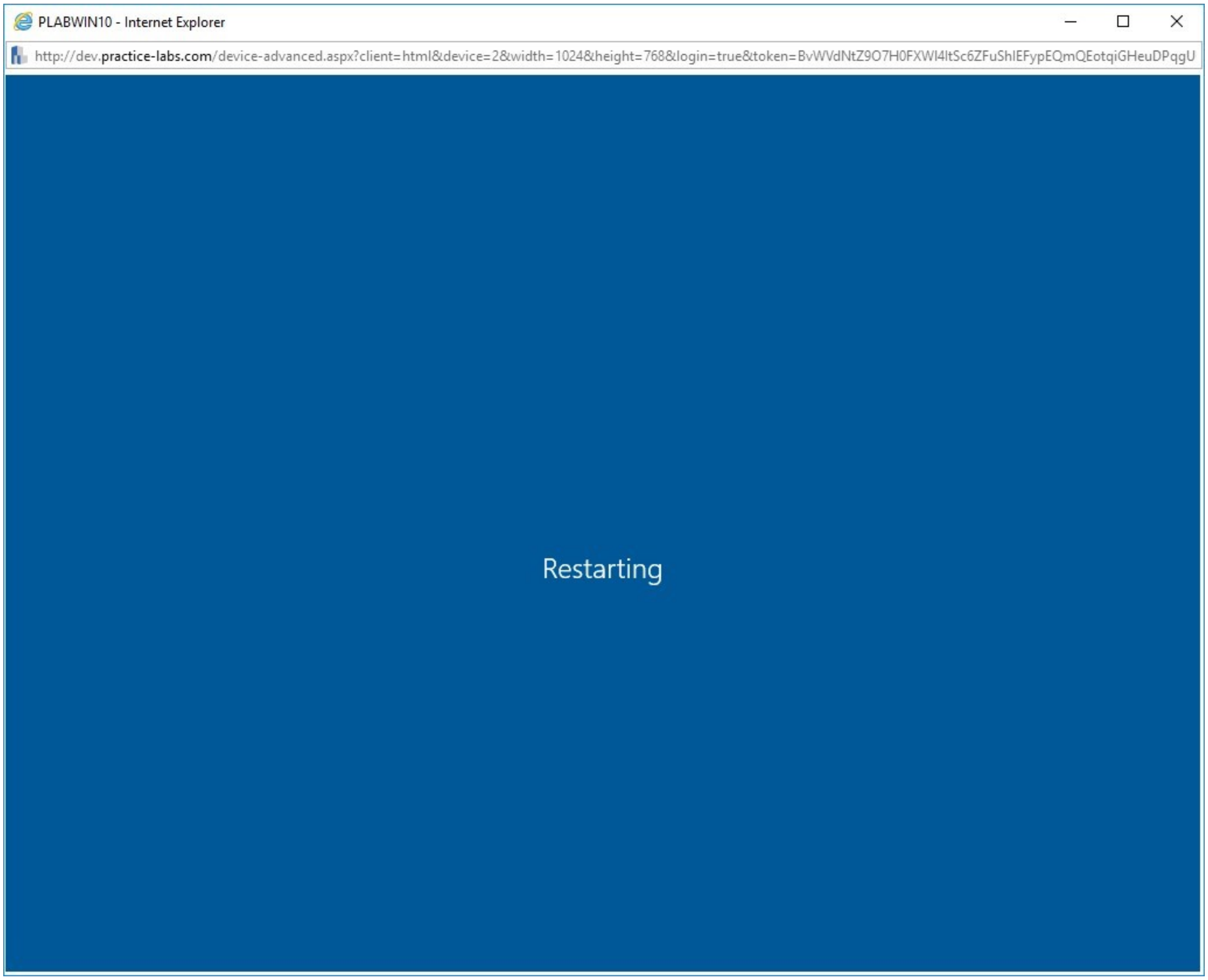
● Yes, restart the computer now

○ No, I will restart the computer later

Figure 1.87 Screenshot of PLABWIN10: Selecting Yes, restart the computer now, and clicking Finish on the completion page.

Step 10

PLABWIN10 will restart.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShIEFypEQmQEotqiGHeuDPqgU

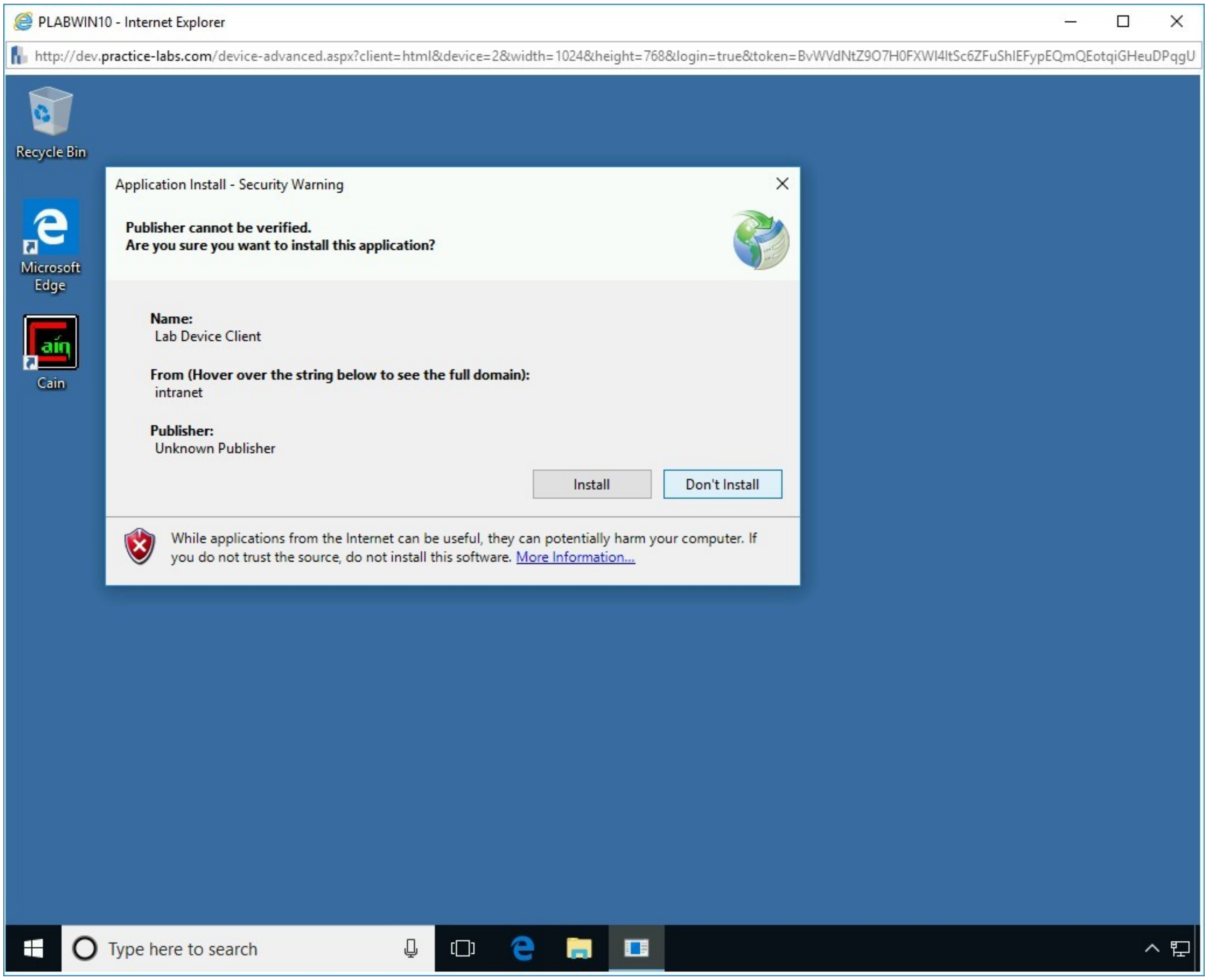
Restarting

Figure 1.88 Screenshot of PLABWIN10: Showing the restart of the PLABWIN10 system.

Step 11

Reconnect to **PLABWIN10** after 1 minute.

The **Application Install - Security Warning** dialog box is displayed. You will be prompted to install the **Lab Device Client**. Click **Don’t Install**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Recycle Bin
Microsoft Edge
Cain
Type here to search

Application Install - Security Warning

Publisher cannot be verified.
Are you sure you want to install this application?

Name:
Lab Device Client

From (Hover over the string below to see the full domain):
intranet

Publisher:
Unknown Publisher

Install | Don't Install

While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. More Information...

Figure 1.89 Screenshot of PLABWIN10: Clicking Don’t Install on the Application Install - Security Warning dialog box.

Step 12

Click the **Windows** charm, scroll down and select **Sniff - O - Matic** folder and then select **Sniff - O - Matic**.

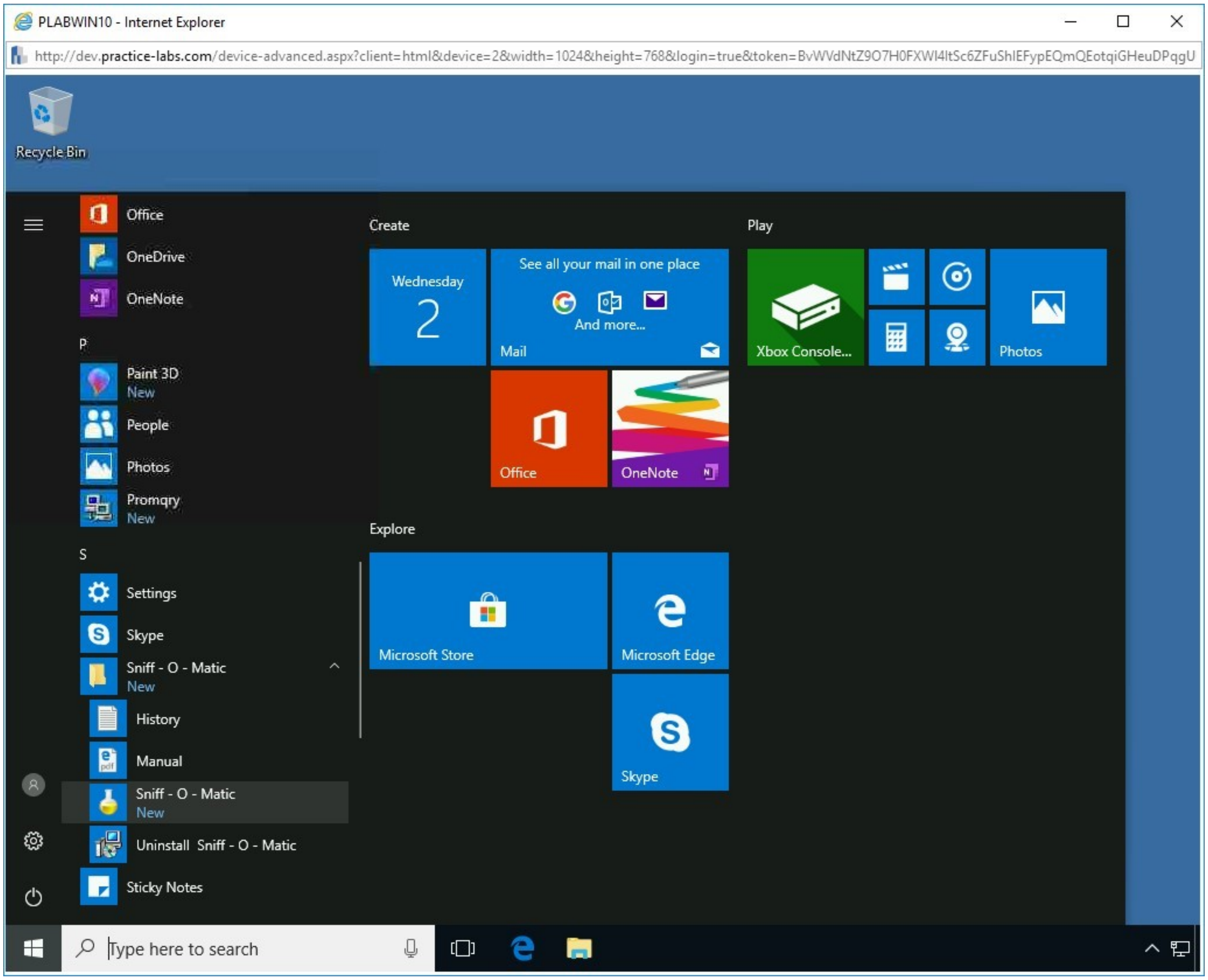
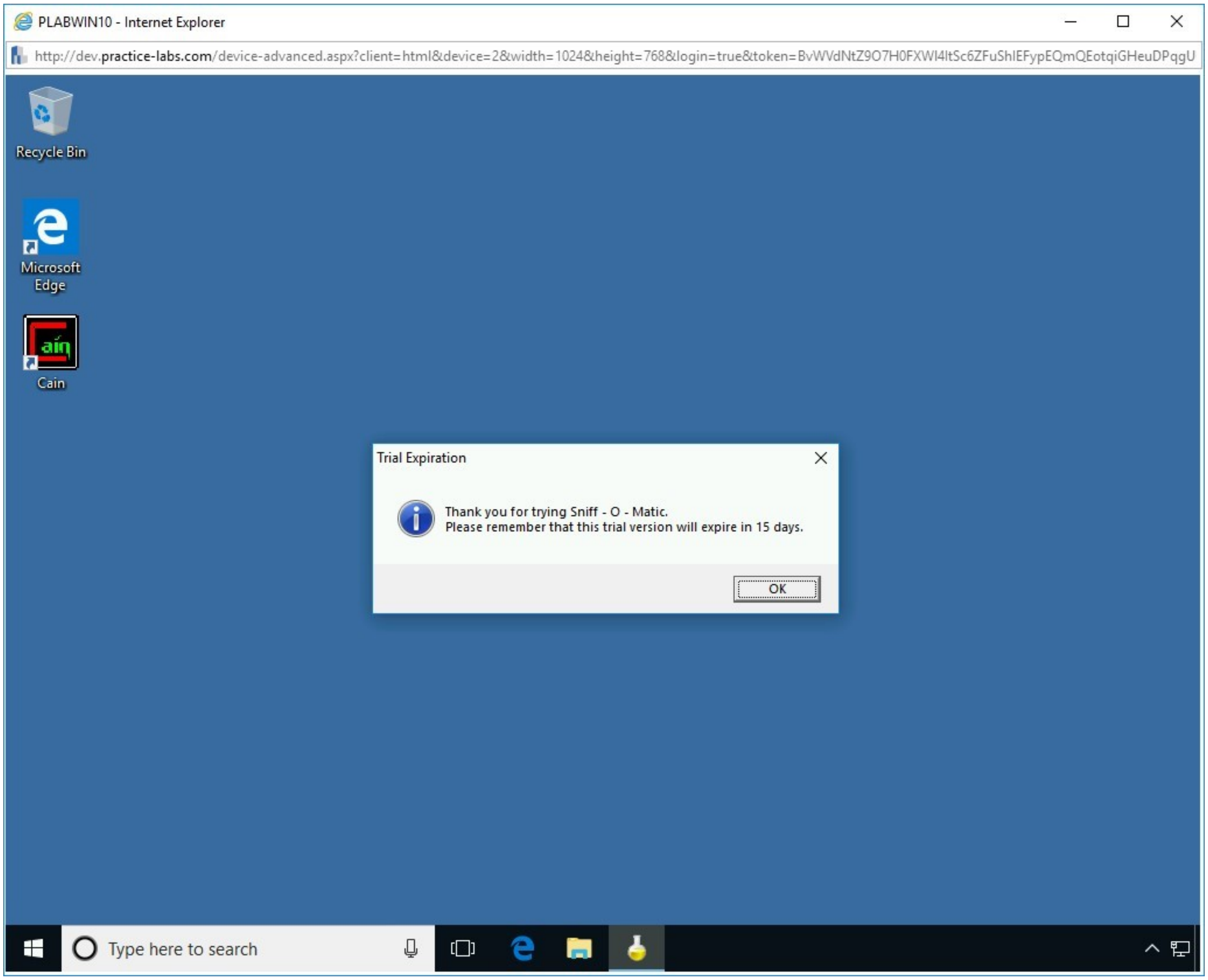


Figure 1.90 Screenshot of PLABWIN10: Selecting Sniff - O - Matic in the Windows menu.

Step 13

If you are using an evaluation version of **Sniff - O - Matic**, then you will be prompted with the **Trial Expiration** dialog box.

Click **OK** to close the dialog box.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShIEFypEQmQEotqiGHeuDPqgU
Recycle Bin
Microsoft Edge
Cain
Type here to search

Trial Expiration

Thank you for trying Sniff - O - Matic.
Please remember that this trial version will expire in 15 days.

OK

Figure 1.91 Screenshot of PLABWIN10: Clicking OK on the Trial Expiration dialog box.

Step 14

The **Sniff - O - Matic 1.07** window is displayed. Click **Start Capture** (the green arrow).

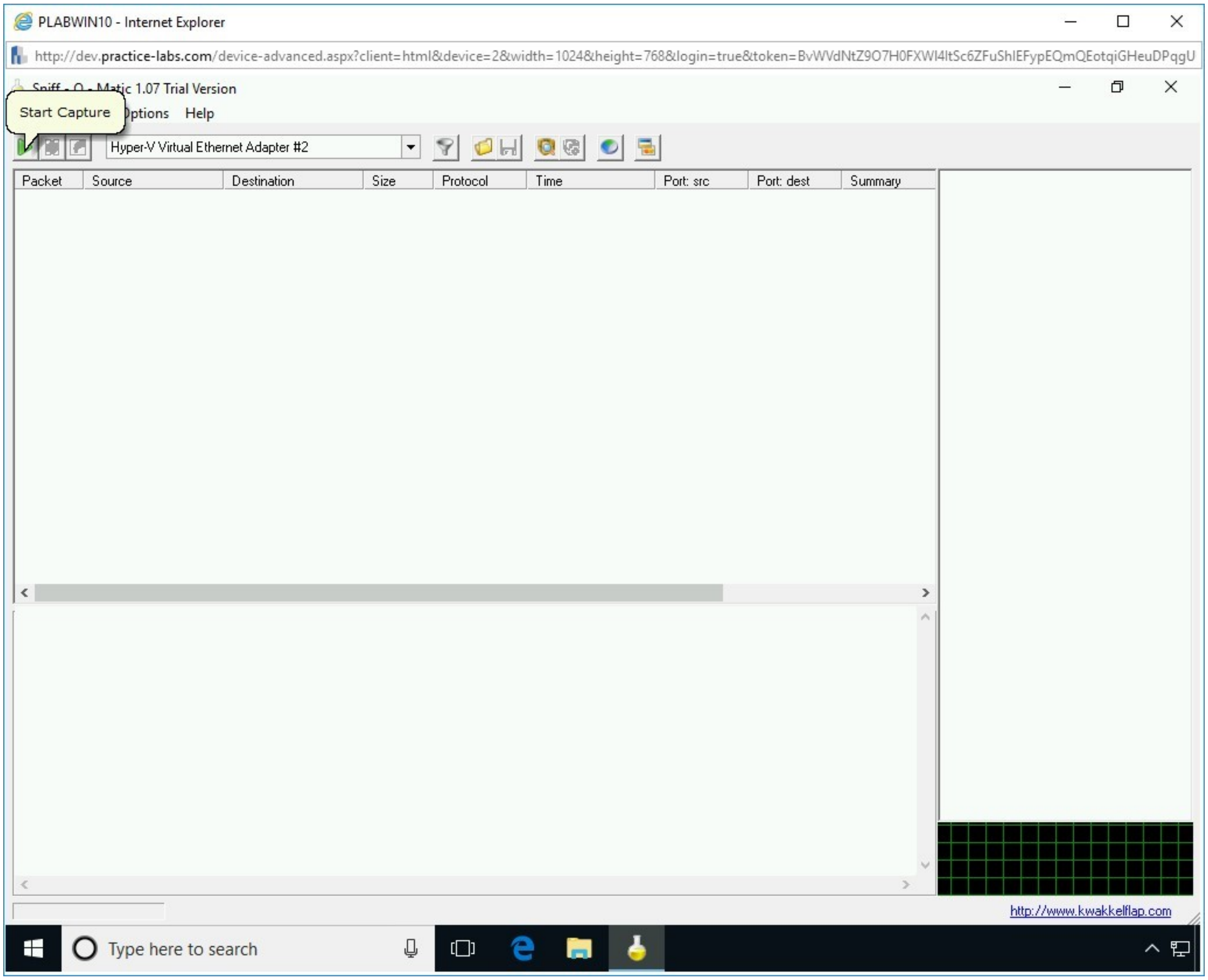
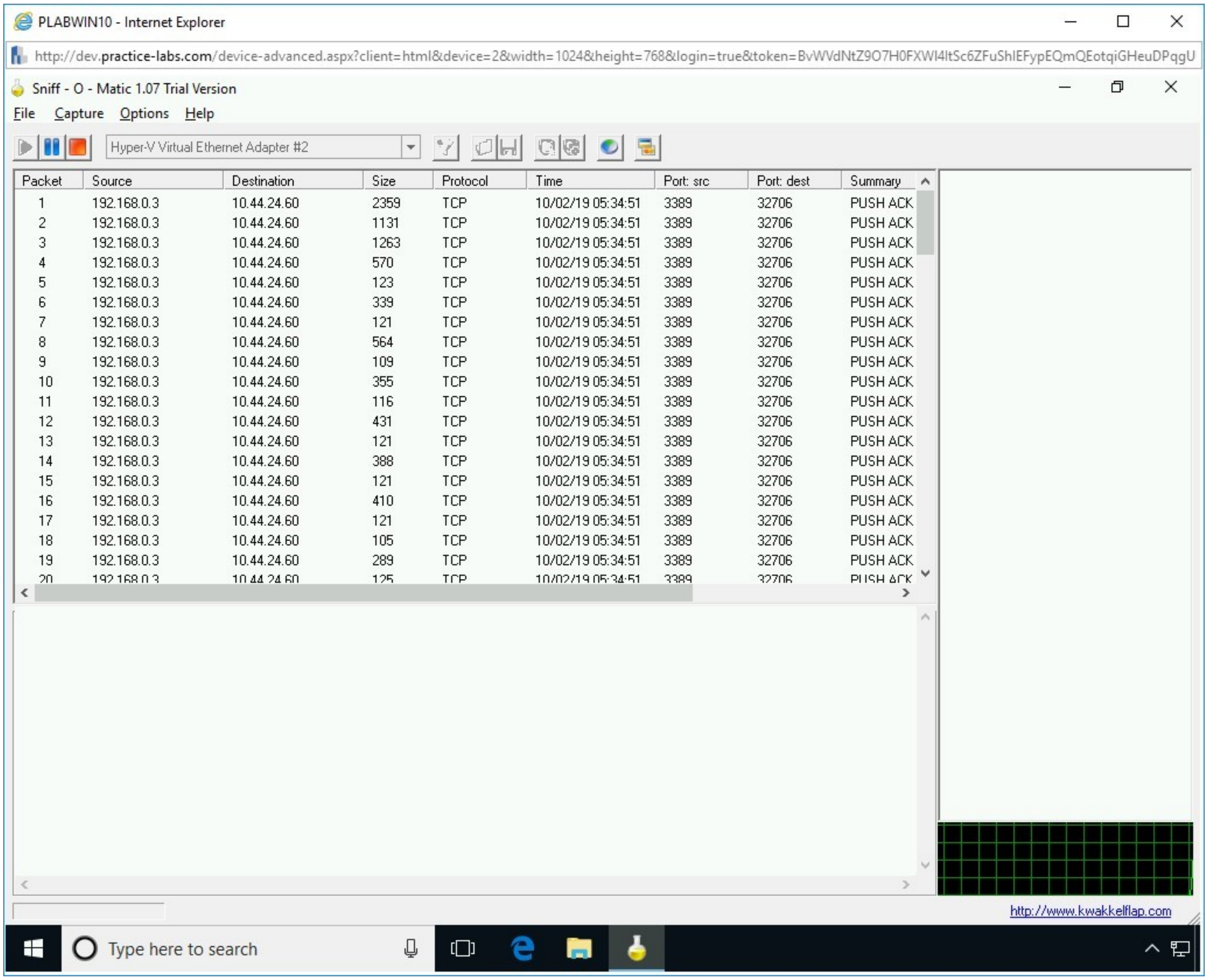

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShIEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
Start Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
Packet
Source
Destination
Size
Protocol
Time
Port: src
Port: dest
Summary
http://www.kwakkelflap.com
Type here to search

Figure 1.92 Screenshot of PLABWIN10: Clicking the Start Capture button (green arrow).

Step 15

The packet capturing process starts.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
http://www.kwakkelflap.com
Type here to search

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port: dest	Summary
1	192.168.0.3	10.44.24.60	2359	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
2	192.168.0.3	10.44.24.60	1131	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
3	192.168.0.3	10.44.24.60	1263	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
4	192.168.0.3	10.44.24.60	570	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
5	192.168.0.3	10.44.24.60	123	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
6	192.168.0.3	10.44.24.60	339	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
7	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
8	192.168.0.3	10.44.24.60	564	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
9	192.168.0.3	10.44.24.60	109	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
10	192.168.0.3	10.44.24.60	355	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
11	192.168.0.3	10.44.24.60	116	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
12	192.168.0.3	10.44.24.60	431	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
13	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
14	192.168.0.3	10.44.24.60	388	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
15	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
16	192.168.0.3	10.44.24.60	410	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
17	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
18	192.168.0.3	10.44.24.60	105	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
19	192.168.0.3	10.44.24.60	289	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
20	192.168.0.3	10.44.24.60	125	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK

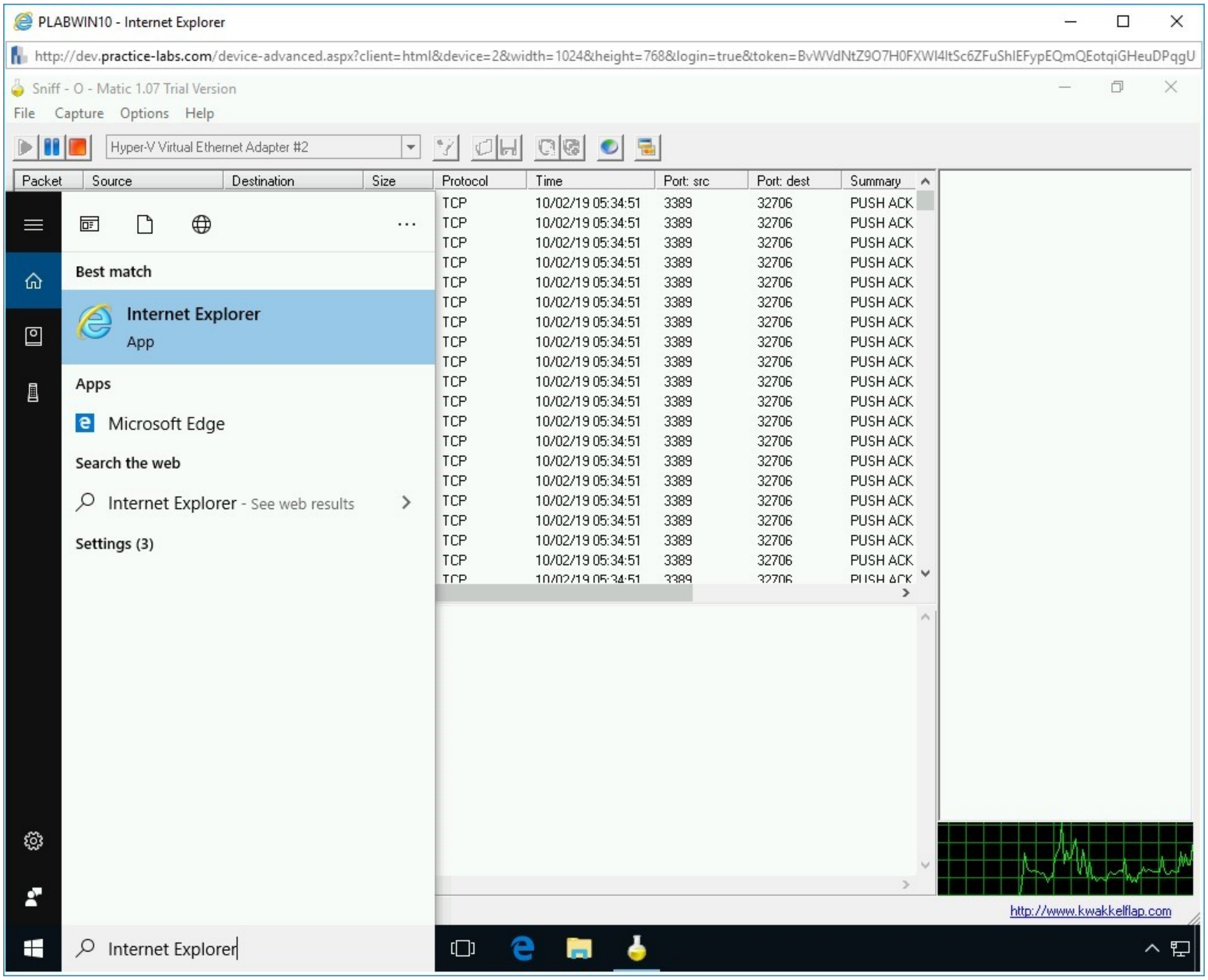
Figure 1.93 Screenshot of PLABWIN10: Showing the packet capture process.

Step 16

In the **Type here to search** text box, type the following:

```
Internet Explorer
```

Select **Internet Explorer** from the search results.

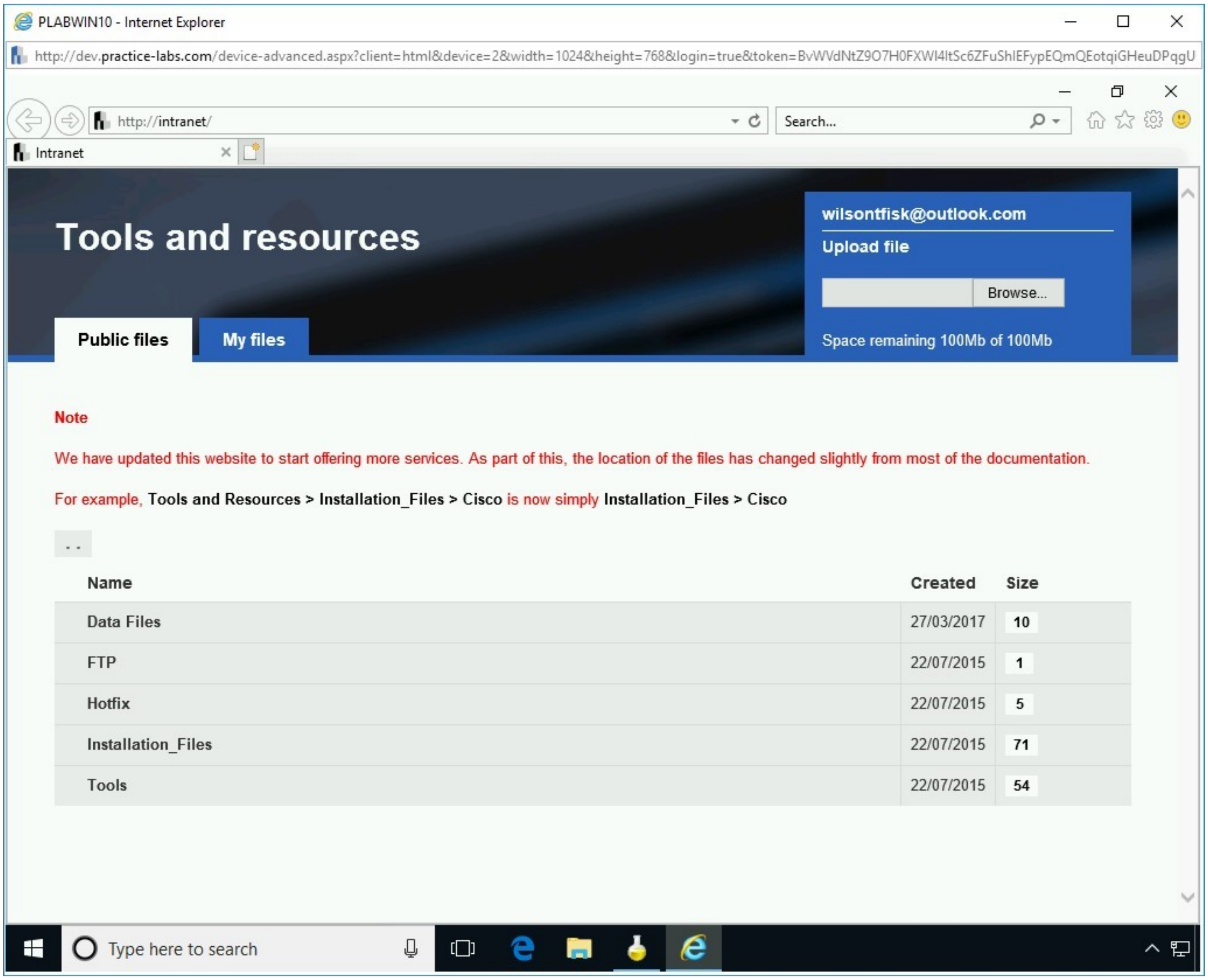

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
Packet
Source
Destination
Size
Best match
Internet Explorer
App
Apps
Microsoft Edge
Search the web
Internet Explorer - See web results
Settings (3)
Internet Explorer
http://www.kwakkelflap.com

Protocol	Time	Port: src	Port: dest	Summary
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
TCP	10/02/19 05:34:51	3389	32706	PUSH ACK

Figure 1.94 Screenshot of PLABWIN10: Selecting Internet Explorer from the search results.

Step 17

The **Intranet** Webpage is displayed.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
http://intranet/
Search...
Intranet
Tools and resources
wilsontfisk@outlook.com
Upload file
Browse...
Space remaining 100Mb of 100Mb
Public files
My files
Type here to search

Note

We have updated this website to start offering more services. As part of this, the location of the files has changed slightly from most of the documentation.

For example, Tools and Resources > Installation_Files > Cisco is now simply Installation_Files > Cisco

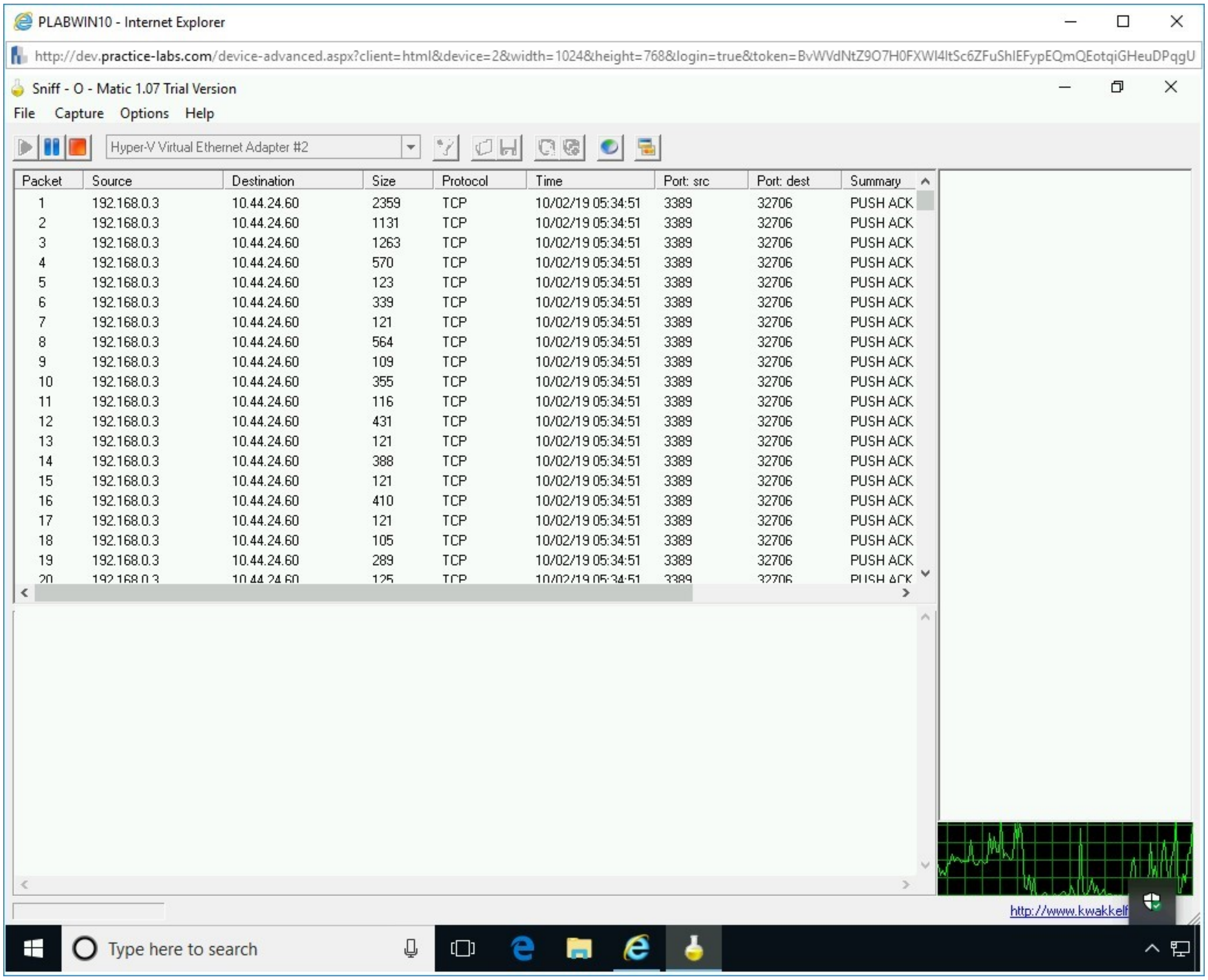
. .

Name	Created	Size
Data Files	27/03/2017	10
FTP	22/07/2015	1
Hotfix	22/07/2015	5
Installation_Files	22/07/2015	71
Tools	22/07/2015	54

Figure 1.95 Screenshot of PLABWIN10: Showing the intranet Webpage.

Step 18

Switch back to **Sniff - O - Matic**.

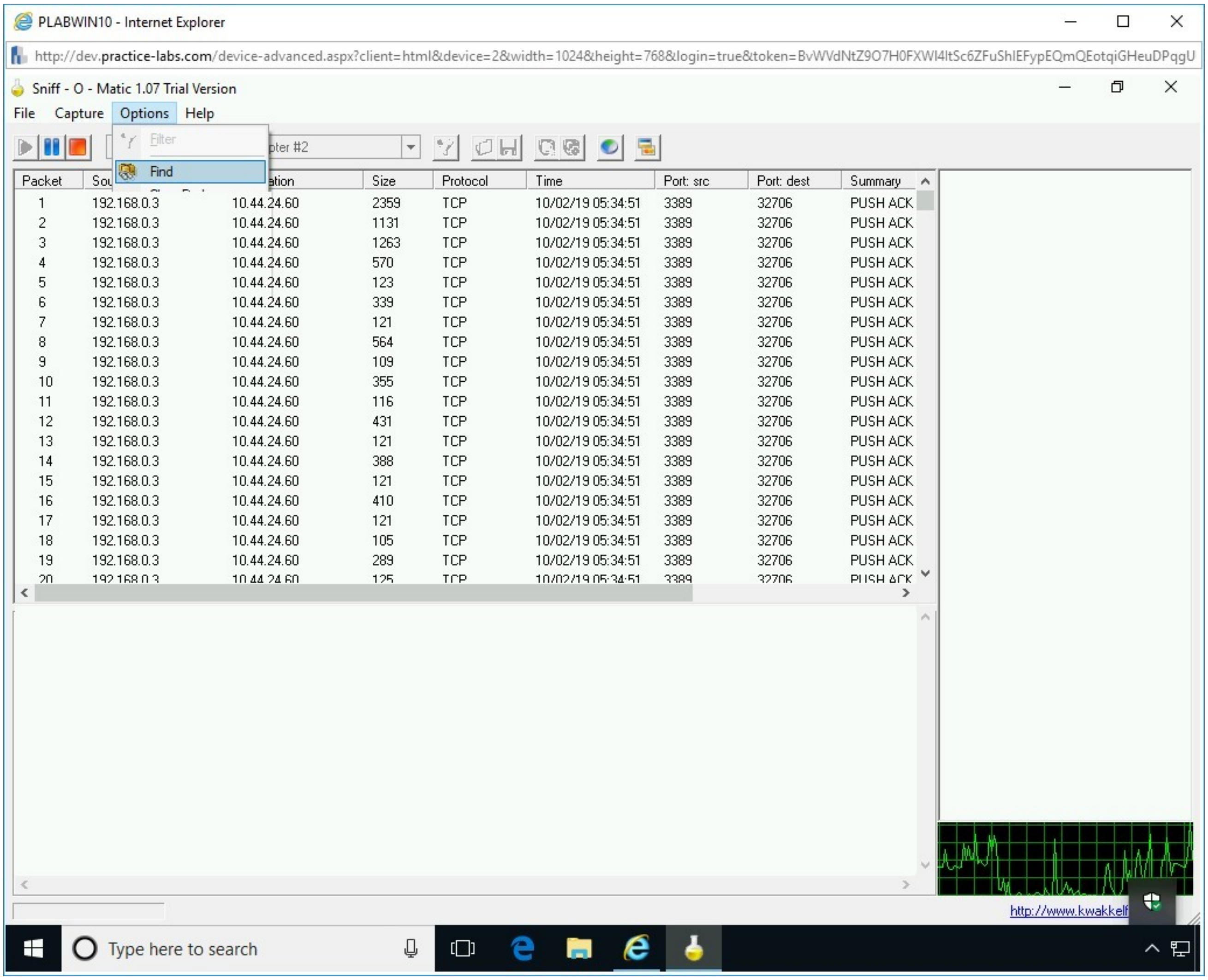

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
http://www.kwakkelf
Type here to search

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port: dest	Summary
1	192.168.0.3	10.44.24.60	2359	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
2	192.168.0.3	10.44.24.60	1131	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
3	192.168.0.3	10.44.24.60	1263	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
4	192.168.0.3	10.44.24.60	570	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
5	192.168.0.3	10.44.24.60	123	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
6	192.168.0.3	10.44.24.60	339	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
7	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
8	192.168.0.3	10.44.24.60	564	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
9	192.168.0.3	10.44.24.60	109	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
10	192.168.0.3	10.44.24.60	355	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
11	192.168.0.3	10.44.24.60	116	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
12	192.168.0.3	10.44.24.60	431	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
13	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
14	192.168.0.3	10.44.24.60	388	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
15	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
16	192.168.0.3	10.44.24.60	410	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
17	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
18	192.168.0.3	10.44.24.60	105	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
19	192.168.0.3	10.44.24.60	289	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
20	192.168.0.3	10.44.24.60	125	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK

Figure 1.96 Screenshot of PLABWIN10: Showing the Sniff - O - Matic window.

Step 19

Click **Options** and select **Find**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShIEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Filter
Find
pter #2
http://www.kwakkelf
Type here to search

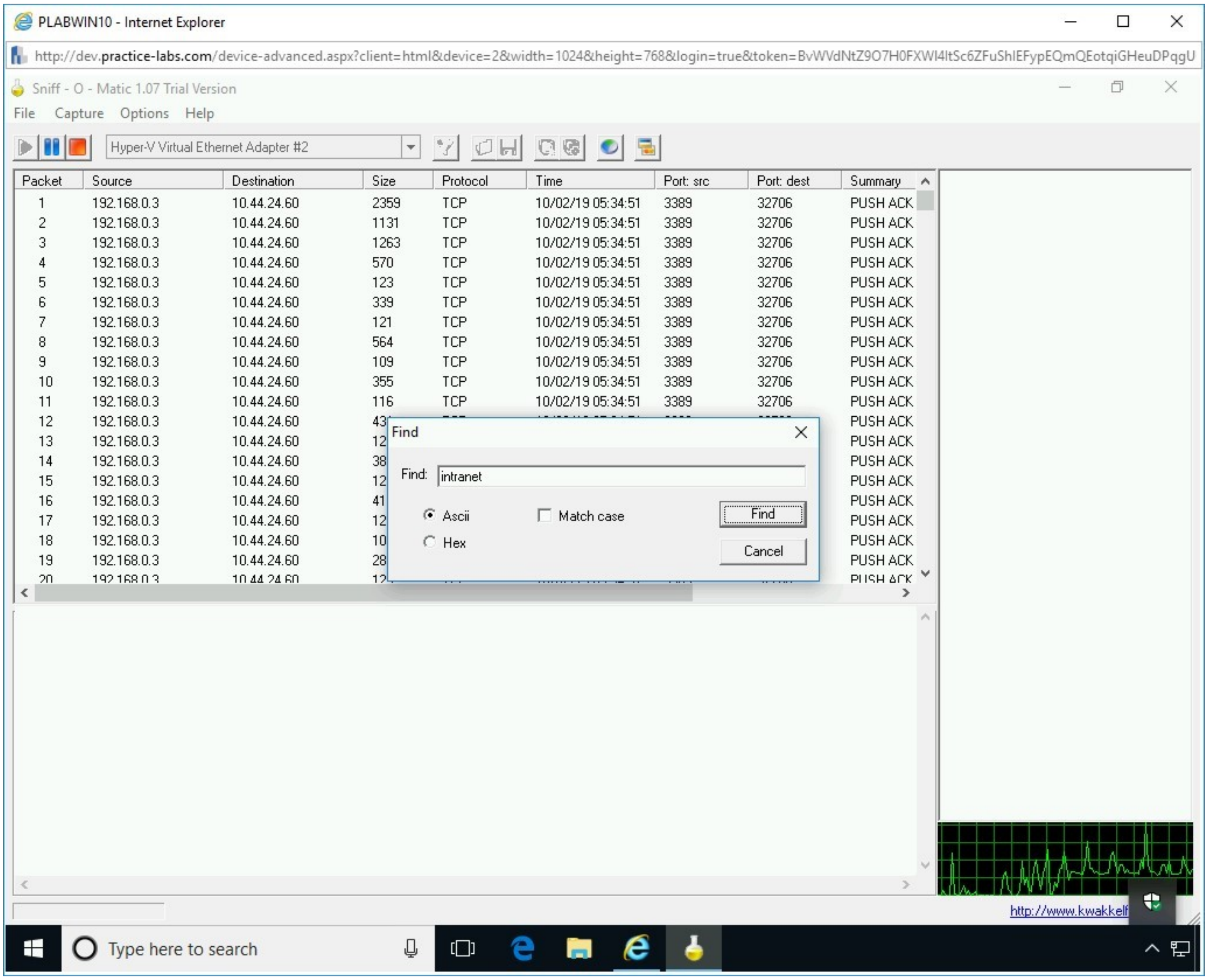
Packet	Sou	ation	Size	Protocol	Time	Port: src	Port: dest	Summary
1	192.168.0.3	10.44.24.60	2359	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
2	192.168.0.3	10.44.24.60	1131	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
3	192.168.0.3	10.44.24.60	1263	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
4	192.168.0.3	10.44.24.60	570	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
5	192.168.0.3	10.44.24.60	123	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
6	192.168.0.3	10.44.24.60	339	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
7	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
8	192.168.0.3	10.44.24.60	564	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
9	192.168.0.3	10.44.24.60	109	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
10	192.168.0.3	10.44.24.60	355	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
11	192.168.0.3	10.44.24.60	116	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
12	192.168.0.3	10.44.24.60	431	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
13	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
14	192.168.0.3	10.44.24.60	388	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
15	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
16	192.168.0.3	10.44.24.60	410	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
17	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
18	192.168.0.3	10.44.24.60	105	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
19	192.168.0.3	10.44.24.60	289	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
20	192.168.0.3	10.44.24.60	125	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK

Figure 1.97 Screenshot of PLABWIN10: Selecting Find from the Options menu.

Step 20

The **Find** dialog box is displayed.

In the **Find** text box, enter **intranet** and click **Find**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
http://www.kwakkelf
Type here to search

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port: dest	Summary
1	192.168.0.3	10.44.24.60	2359	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
2	192.168.0.3	10.44.24.60	1131	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
3	192.168.0.3	10.44.24.60	1263	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
4	192.168.0.3	10.44.24.60	570	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
5	192.168.0.3	10.44.24.60	123	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
6	192.168.0.3	10.44.24.60	339	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
7	192.168.0.3	10.44.24.60	121	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
8	192.168.0.3	10.44.24.60	564	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
9	192.168.0.3	10.44.24.60	109	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
10	192.168.0.3	10.44.24.60	355	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
11	192.168.0.3	10.44.24.60	116	TCP	10/02/19 05:34:51	3389	32706	PUSH ACK
12	192.168.0.3	10.44.24.60	43					PUSH ACK
13	192.168.0.3	10.44.24.60	12					PUSH ACK
14	192.168.0.3	10.44.24.60	38					PUSH ACK
15	192.168.0.3	10.44.24.60	12					PUSH ACK
16	192.168.0.3	10.44.24.60	41					PUSH ACK
17	192.168.0.3	10.44.24.60	12					PUSH ACK
18	192.168.0.3	10.44.24.60	10					PUSH ACK
19	192.168.0.3	10.44.24.60	28					PUSH ACK
20	192.168.0.3	10.44.24.60	12					PUSH ACK

Find

Find: intranet

● Ascii

○ Hex

□ Match case

Find

Cancel

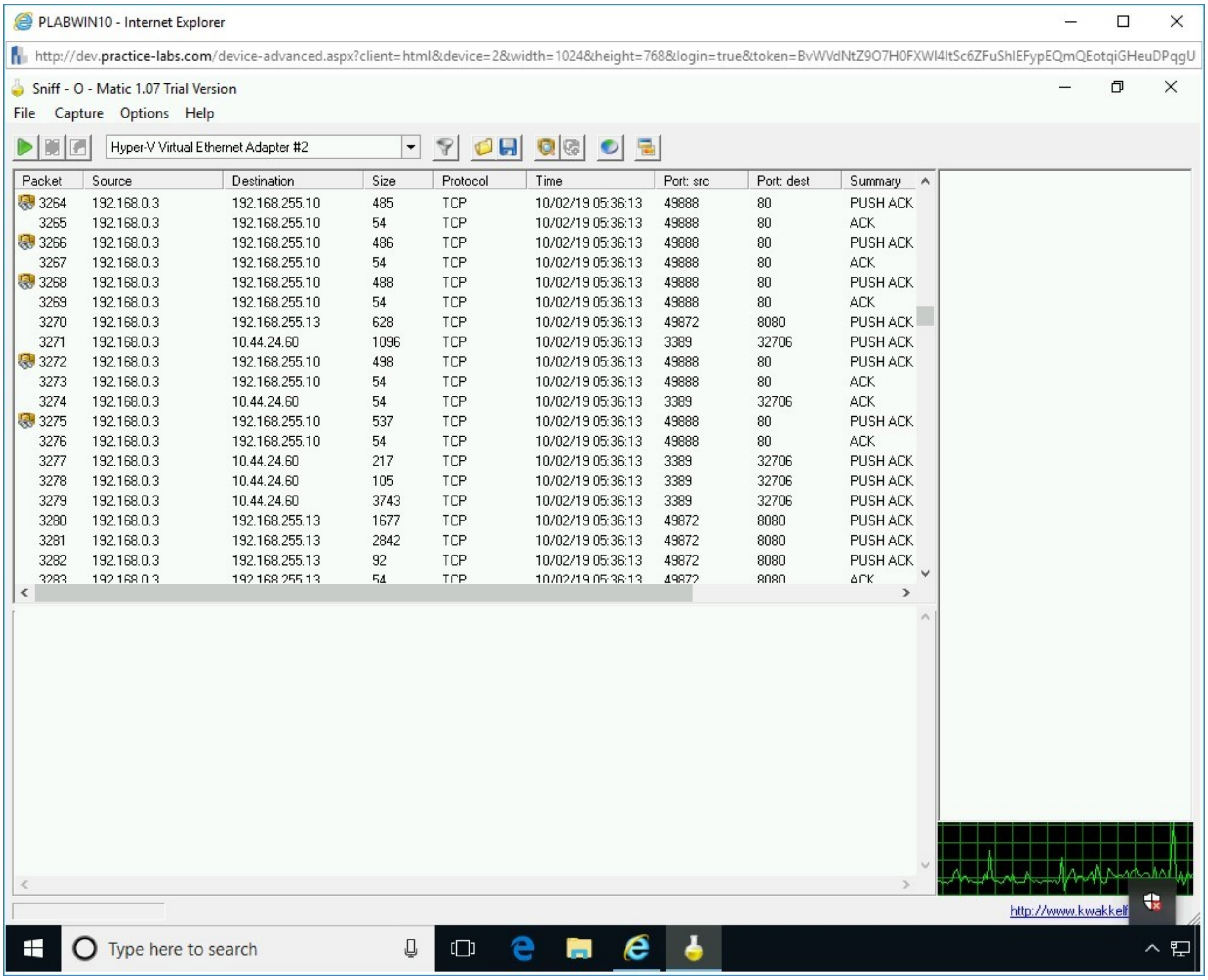
Figure 1.98 Screenshot of PLABWIN10: Entering intranet in the Find text box, leaving Ascii selected and clicking Find.

Step 21

You may need to scroll down the captured data packets to find the result.

Note that one result has been located. The packet with the keyword “**intranet**” will be marked with the **binoculars** icon.

> ***Note:*** *Since there will be thousands of sniffed packets, you may have to scroll either up or down to find the relevant results.*



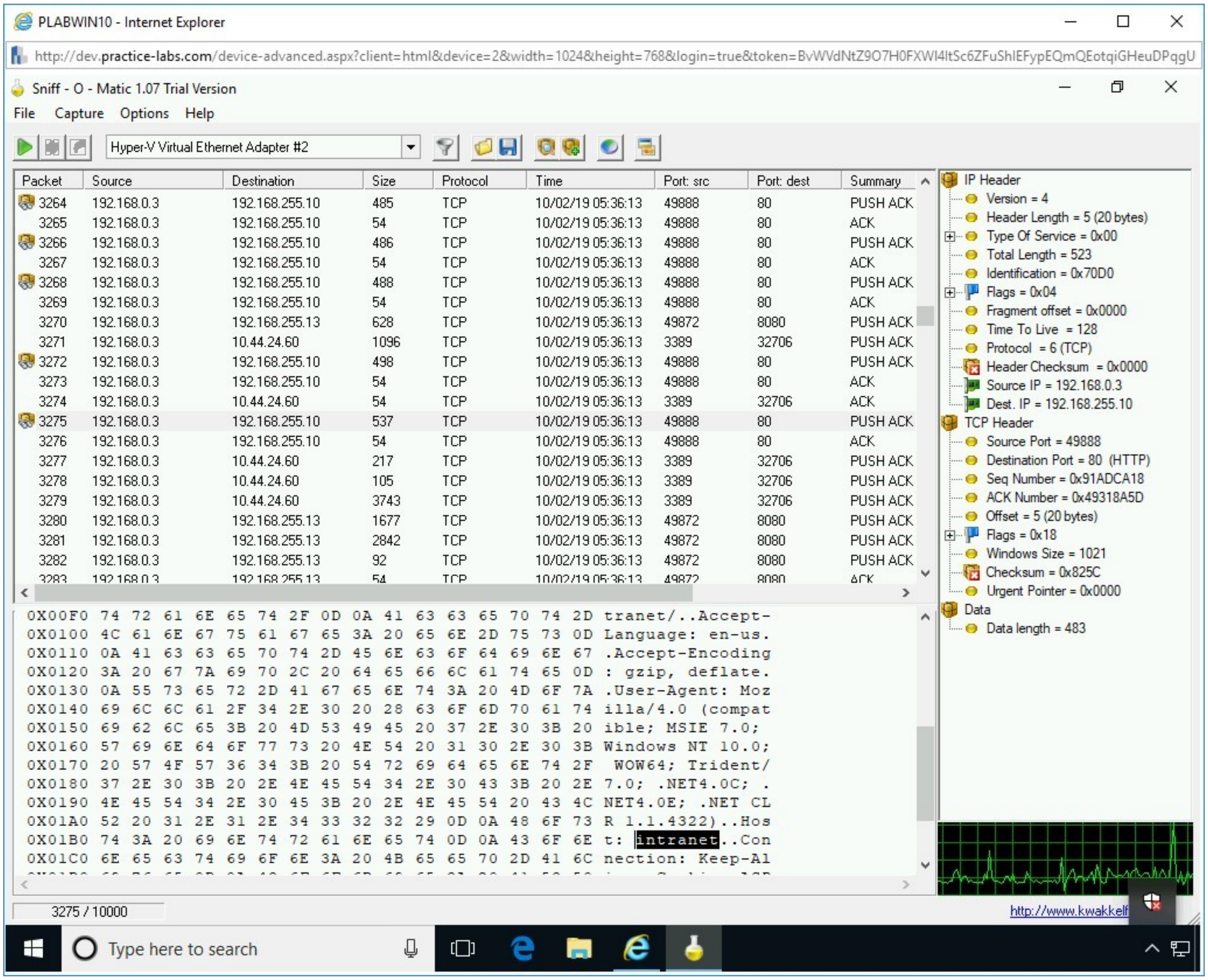
PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWI4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File Capture Options Help
Hyper-V Virtual Ethernet Adapter #2
http://www.kwakkelf
Type here to search

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port: dest	Summary
3264	192.168.0.3	192.168.255.10	485	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3265	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3266	192.168.0.3	192.168.255.10	486	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3267	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3268	192.168.0.3	192.168.255.10	488	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3269	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3270	192.168.0.3	192.168.255.13	628	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3271	192.168.0.3	10.44.24.60	1096	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3272	192.168.0.3	192.168.255.10	498	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3273	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3274	192.168.0.3	10.44.24.60	54	TCP	10/02/19 05:36:13	3389	32706	ACK
3275	192.168.0.3	192.168.255.10	537	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3276	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3277	192.168.0.3	10.44.24.60	217	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3278	192.168.0.3	10.44.24.60	105	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3279	192.168.0.3	10.44.24.60	3743	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3280	192.168.0.3	192.168.255.13	1677	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3281	192.168.0.3	192.168.255.13	2842	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3282	192.168.0.3	192.168.255.13	92	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3283	192.168.0.3	192.168.255.13	54	TCP	10/02/19 05:36:13	49872	8080	ACK

Figure 1.99 Screenshot of PLABWIN10: Showing the search results.

Step 22

You can find the details of this packet on the hexadecimal pane.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=BvWVdNtZ9O7H0FXWl4ltSc6ZFuShlEFypEQmQEotqiGHeuDPqgU
Sniff - O - Matic 1.07 Trial Version
File
Capture
Options
Help
Hyper-V Virtual Ethernet Adapter #2
3275 / 10000
http://www.kwakkelf
Type here to search

Packet	Source	Destination	Size	Protocol	Time	Port: src	Port: dest	Summary
3264	192.168.0.3	192.168.255.10	485	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3265	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3266	192.168.0.3	192.168.255.10	486	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3267	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3268	192.168.0.3	192.168.255.10	488	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3269	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3270	192.168.0.3	192.168.255.13	628	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3271	192.168.0.3	10.44.24.60	1096	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3272	192.168.0.3	192.168.255.10	498	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3273	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3274	192.168.0.3	10.44.24.60	54	TCP	10/02/19 05:36:13	3389	32706	ACK
3275	192.168.0.3	192.168.255.10	537	TCP	10/02/19 05:36:13	49888	80	PUSH ACK
3276	192.168.0.3	192.168.255.10	54	TCP	10/02/19 05:36:13	49888	80	ACK
3277	192.168.0.3	10.44.24.60	217	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3278	192.168.0.3	10.44.24.60	105	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3279	192.168.0.3	10.44.24.60	3743	TCP	10/02/19 05:36:13	3389	32706	PUSH ACK
3280	192.168.0.3	192.168.255.13	1677	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3281	192.168.0.3	192.168.255.13	2842	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3282	192.168.0.3	192.168.255.13	92	TCP	10/02/19 05:36:13	49872	8080	PUSH ACK
3283	192.168.0.3	192.168.255.13	54	TCP	10/02/19 05:36:13	49872	8080	ACK

```
0X00F0 74 72 61 6E 65 74 2F 0D 0A 41 63 63 65 70 74 2D tranet/..Accept-
0X0100 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 75 73 0D Language: en-us.
0X0110 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 6E 67 .Accept-Encoding
0X0120 3A 20 67 7A 69 70 2C 20 64 65 66 6C 61 74 65 0D : gzip, deflate.
0X0130 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F 7A .User-Agent: Moz
0X0140 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61 74 illa/4.0 (compat
0X0150 69 62 6C 65 3B 20 4D 53 49 45 20 37 2E 30 3B 20 ible; MSIE 7.0;
0X0160 57 69 6E 64 6F 77 73 20 4E 54 20 31 30 2E 30 3B Windows NT 10.0;
0X0170 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F  WOW64; Trident/
0X0180 37 2E 30 3B 20 2E 4E 45 54 34 2E 30 43 3B 20 2E 7.0; .NET4.0C; .
0X0190 4E 45 54 34 2E 30 45 3B 20 2E 4E 45 54 20 43 4C NET4.0E; .NET CL
0X01A0 52 20 31 2E 31 2E 34 33 32 32 29 0D 0A 48 6F 73 R 1.1.4322)..Hos
0X01B0 74 3A 20 69 6E 74 72 61 6E 65 74 0D 0A 43 6F 6E t: intranet..Con
0X01C0 6E 65 63 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C nection: Keep-Al
```

- IP Header
  - Version = 4
  - Header Length = 5 (20 bytes)
  - Type Of Service = 0x00
  - Total Length = 523
  - Identification = 0x70D0
  - Flags = 0x04
  - Fragment offset = 0x0000
  - Time To Live = 128
  - Protocol = 6 (TCP)
  - Header Checksum = 0x0000
  - Source IP = 192.168.0.3
  - Dest. IP = 192.168.255.10
- TCP Header
  - Source Port = 49888
  - Destination Port = 80 (HTTP)
  - Seq Number = 0x91ADCA18
  - ACK Number = 0x49318A5D
  - Offset = 5 (20 bytes)
  - Flags = 0x18
  - Windows Size = 1021
  - Checksum = 0x825C
  - Urgent Pointer = 0x0000
- Data
  - Data length = 483

Figure 1.100 Screenshot of PLABWIN10: Showing the details of this packet on the hexadecimal pane.

Close **Sniff-O-Matic** when done.

Exercise 2 - Sniffing Prevention Techniques

There are various methods that can be used against sniffing, which usually takes place with the use of weak protocols, such as HTTP and FTP. You can follow a few simple rules to avoid sniffing:

- Avoid using HTTP and use HTTPS instead
- Avoid using FTP and use SFTP instead
- Avoid using a hub and use a switch instead

- Configure DHCP Snooping
- Configure Dynamic ARP inspection
- Configure Source guard
- Use a tool like XArp to detect ARP-based attacks
- Use a sniffing detection tool to detect a network adapter working in promiscuous mode
- Use appropriate encryption

In this exercise, you will learn to prevent sniffing attacks.

Learning Outcomes

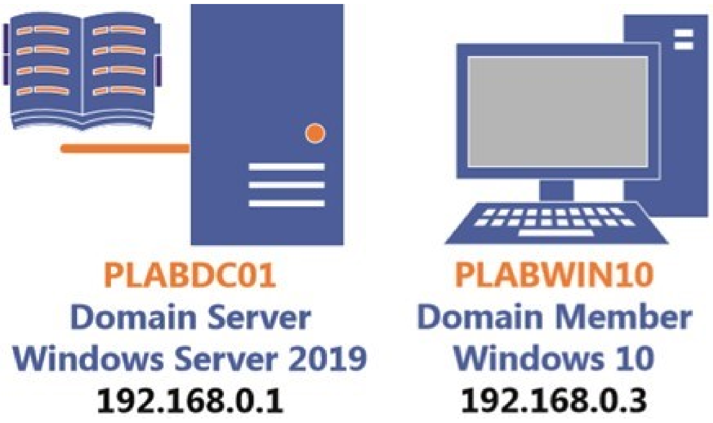
After completing this exercise, you will be able to:

- Use XArp utility

Your Devices

You will be using the following devices in this lab. Please power these on now.

- **PLABDC01 -** (Windows Server 2019 - Domain Server)
- **PLABWIN10 -** (Windows 10 - Workstation)



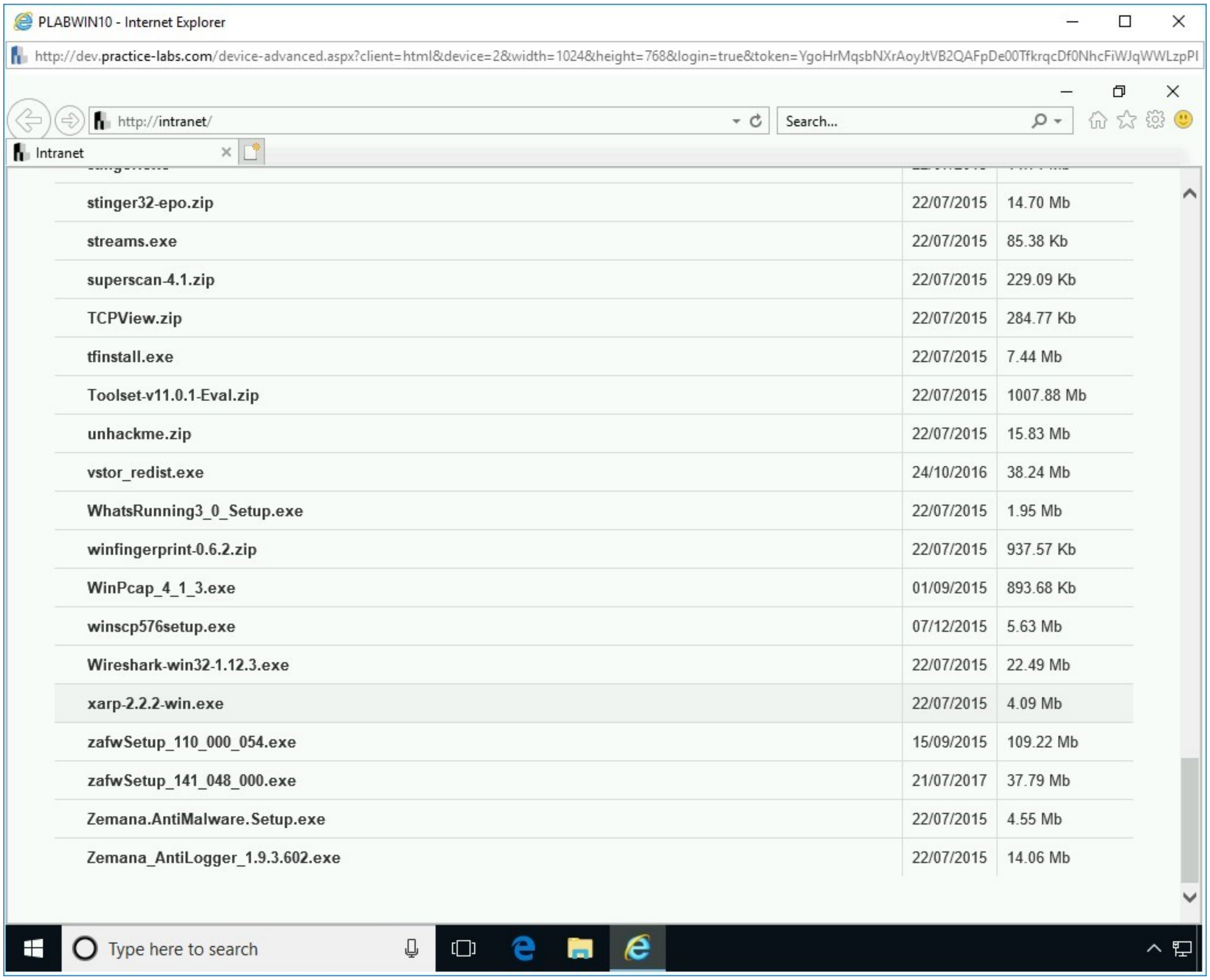
Task 1 - Use XArp Utility

XArp helps you detect an ARP-based attack. It can use active or passive methods to detect the ARP-based attacks on a network. It can perform network monitoring to perform ARP spoofing detection.

In this task, you will learn to use XArp. To use XArp, perform the following steps:

Step 1

Ensure you have powered on all the devices listed in the introduction and connect to **PLABWIN10**. Restore Internet Explorer from the taskbar. You should be on the **Hacking Tools** page. Locate **xarp-2.2.2-win.exe**, and then click on it.



PLABWIN10 - Internet Explorer

http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

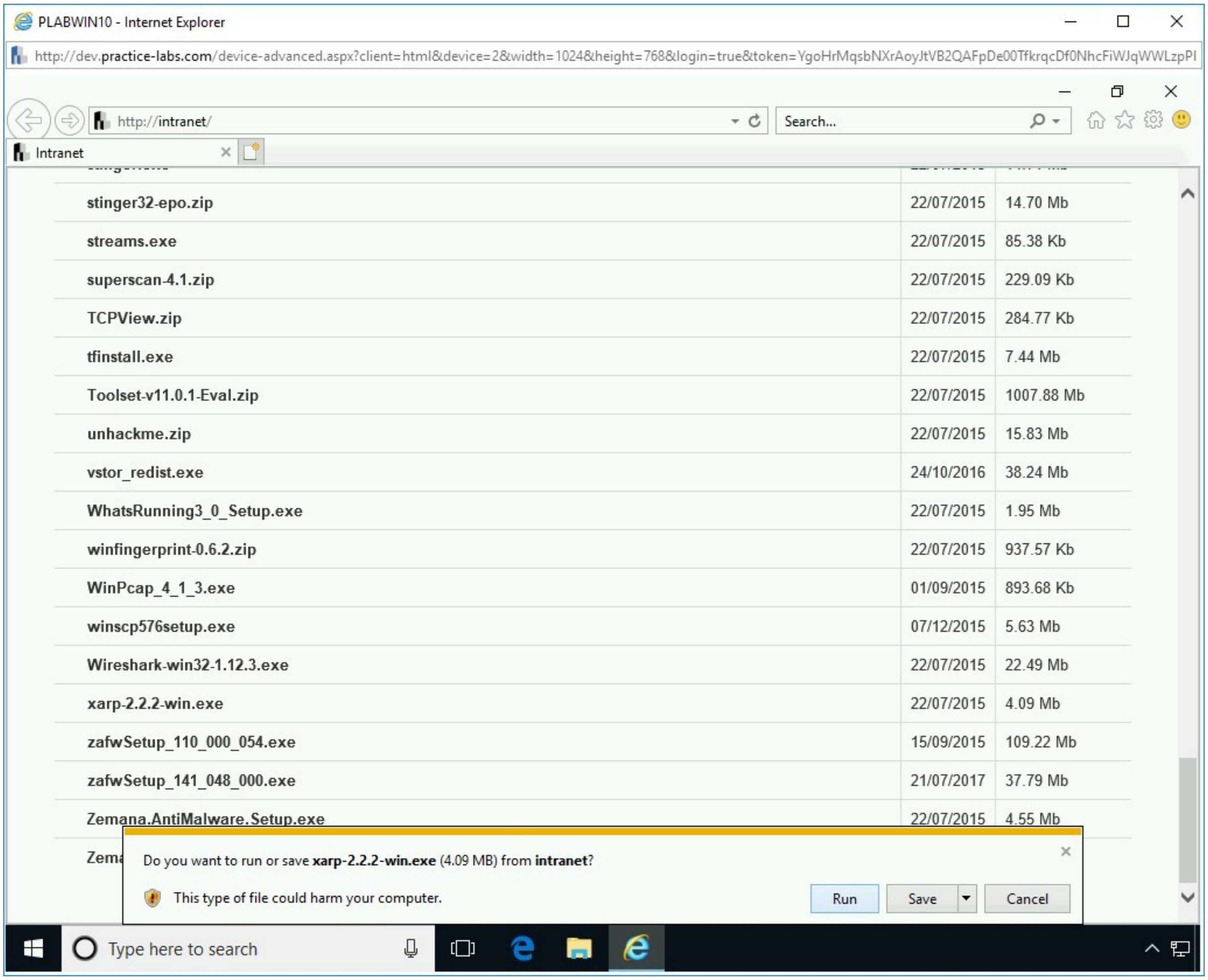
http://intranet/

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

Figure 2.1 Screenshot of PLABWIN10: Clicking the xarp-2.2.2-win.exe file.

Step 2

In the notification bar, click **Run**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zema		

Do you want to run or save **xarp-2.2.2-win.exe** (4.09 MB) from **intranet**?

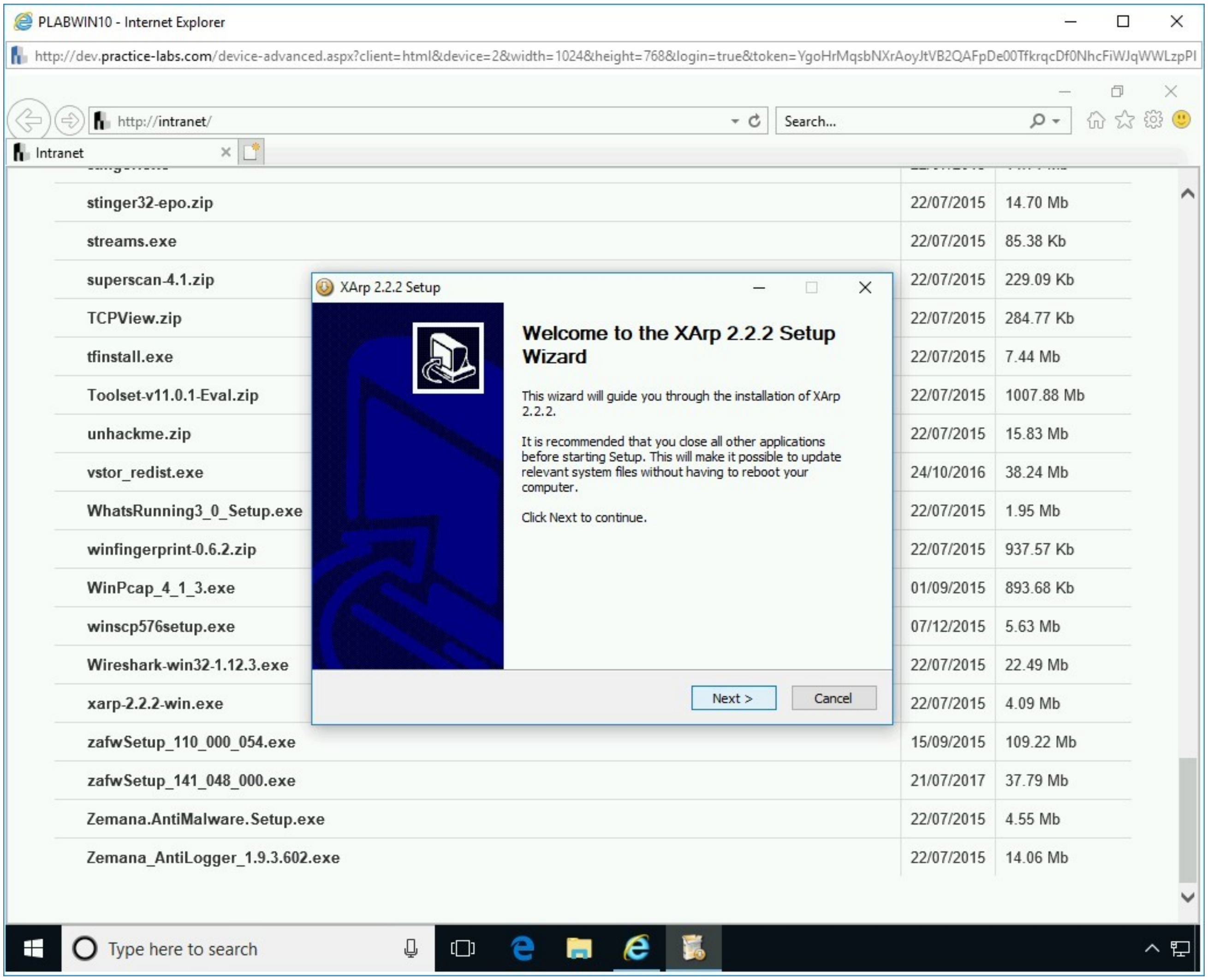
This type of file could harm your computer.

Run | Save | Cancel

Figure 2.2 Screenshot of PLABWIN10: Clicking Run on the notification bar.

Step 3

The **XArp 2.2.2 Setup** wizard is displayed. On the **Welcome to the XArp 2.2.2 Setup Wizard** dialog box, click **Next**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

XArp 2.2.2 Setup

Welcome to the XArp 2.2.2 Setup Wizard

This wizard will guide you through the installation of XArp 2.2.2.

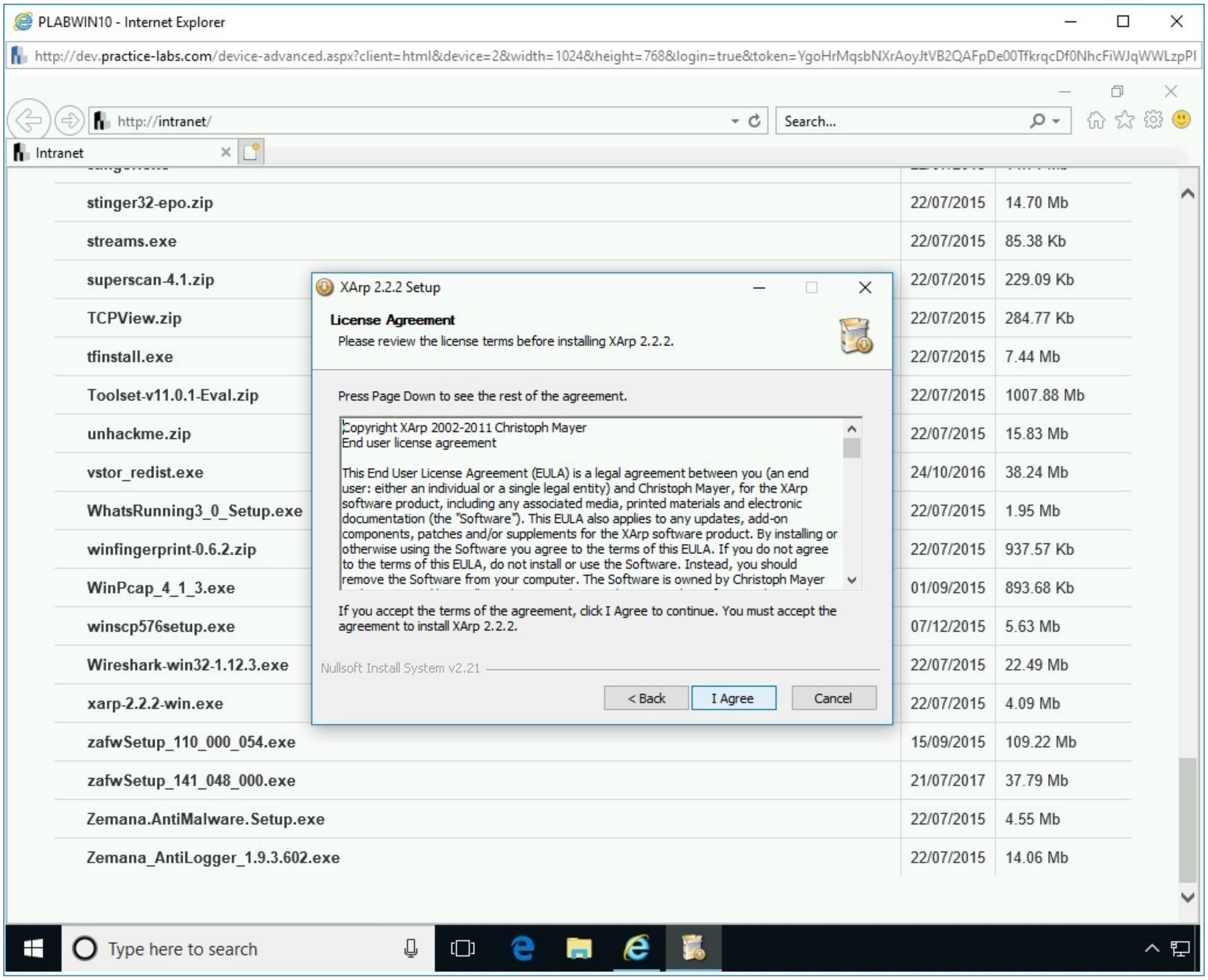
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 2.3 Screenshot of PLABWIN10: Showing the welcome page of the XArp 2.2.2 Setup wizard.

Step 4

On the **License Agreement** page, click **I Agree**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

XArp 2.2.2 Setup

License Agreement

Please review the license terms before installing XArp 2.2.2.

Press Page Down to see the rest of the agreement.

Copyright XArp 2002-2011 Christoph Mayer
End user license agreement

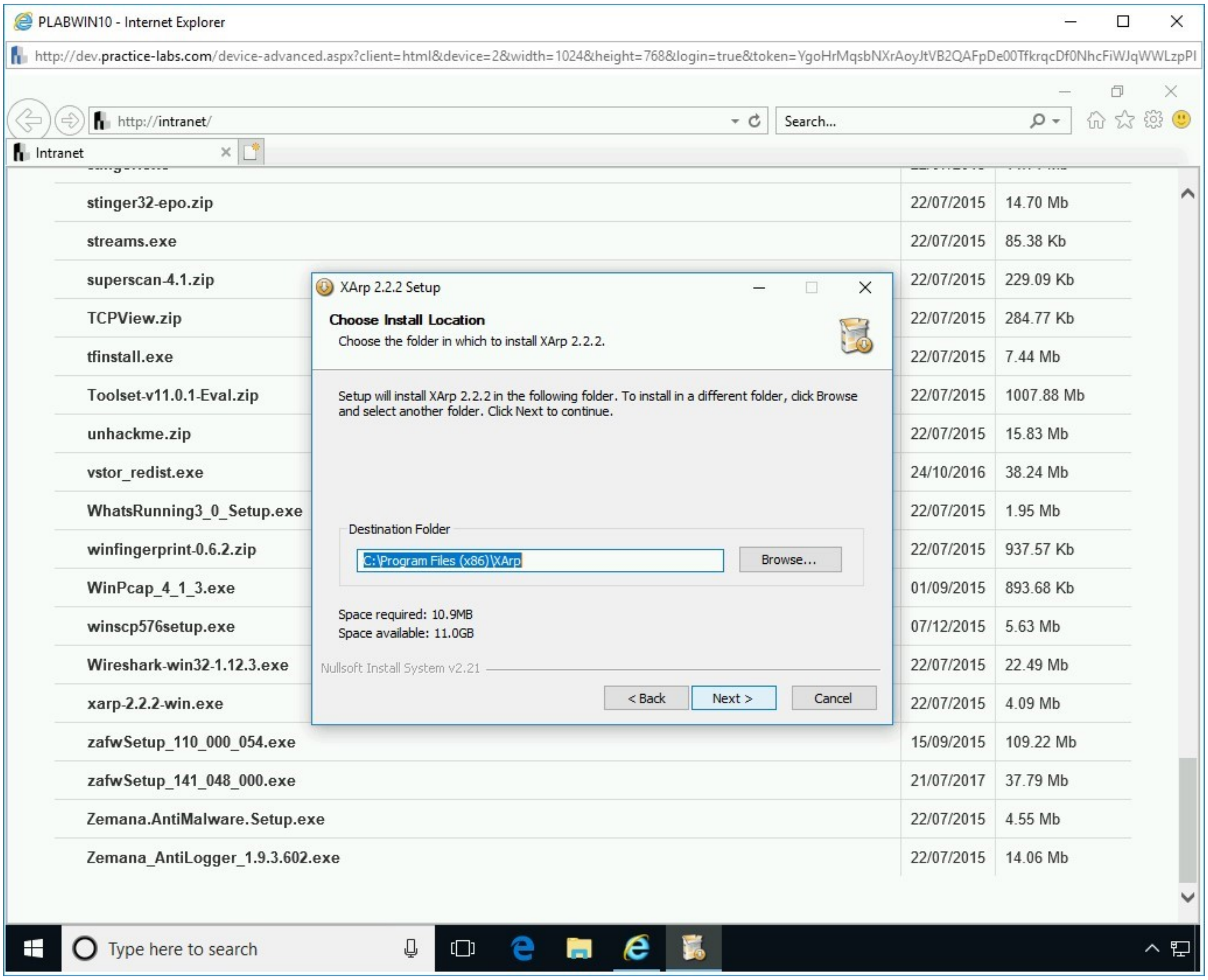
This End User License Agreement (EULA) is a legal agreement between you (an end user: either an individual or a single legal entity) and Christoph Mayer, for the XArp software product, including any associated media, printed materials and electronic documentation (the "Software"). This EULA also applies to any updates, add-on components, patches and/or supplements for the XArp software product. By installing or otherwise using the Software you agree to the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the Software. Instead, you should remove the Software from your computer. The Software is owned by Christoph Mayer

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install XArp 2.2.2.

Figure 2.4 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 5

On the **Choose Install Location** page, keep the default location and click **Next**.



http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl

http://intranet/

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

XArp 2.2.2 Setup

Choose Install Location

Choose the folder in which to install XArp 2.2.2.

Setup will install XArp 2.2.2 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\Program Files (x86)\XArp

Space required: 10.9MB
Space available: 11.0GB

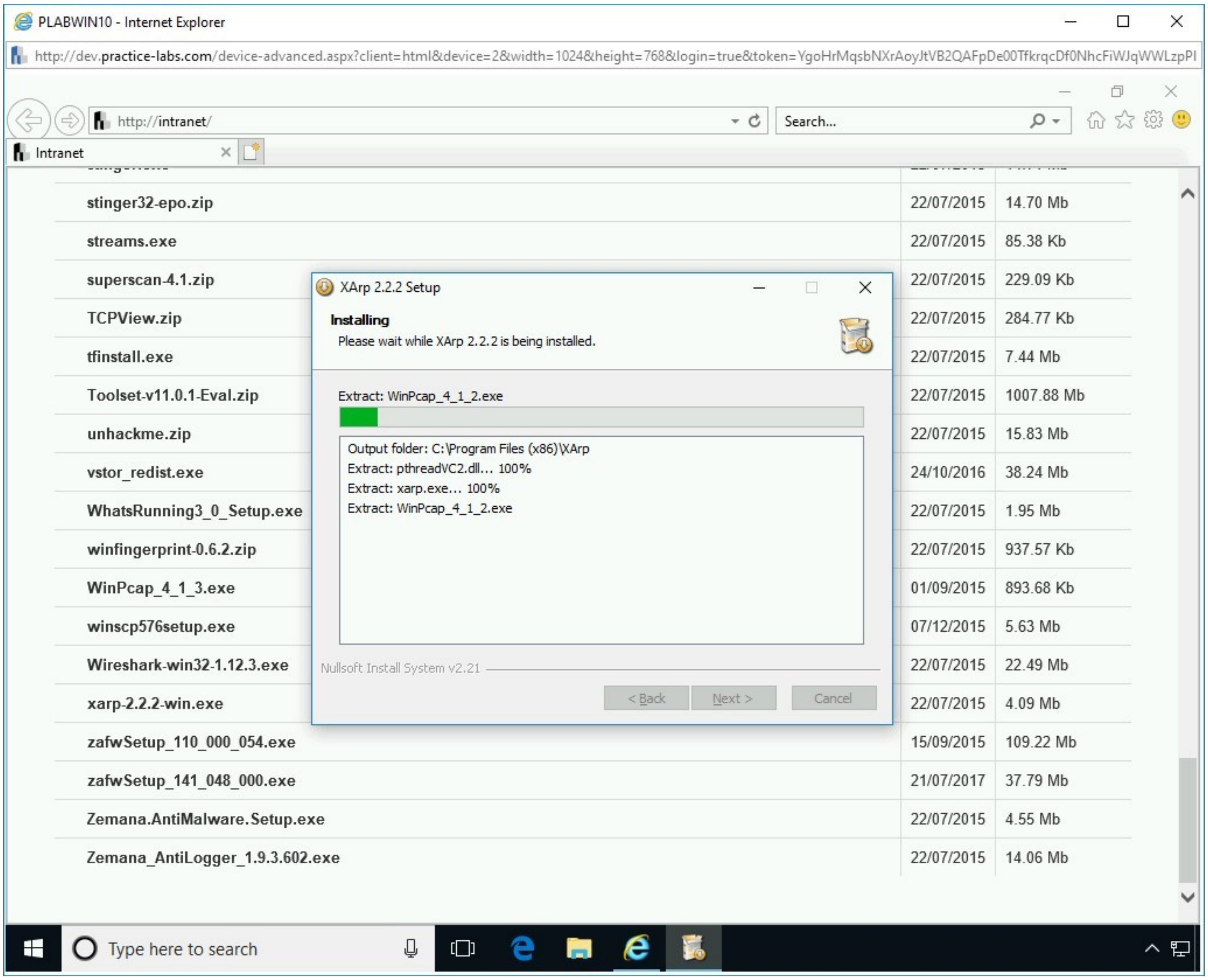
Nullsoft Install System v2.21

Figure 2.5 Screenshot of PLABWIN10: Keeping the default installation location and clicking Next.

Step 6

On the **Choose Start Menu Folder** page, keep the default menu name, and click **Install**.

The installation process starts.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

XArp 2.2.2 Setup

Installing

Please wait while XArp 2.2.2 is being installed.

Extract: WinPcap_4_1_2.exe

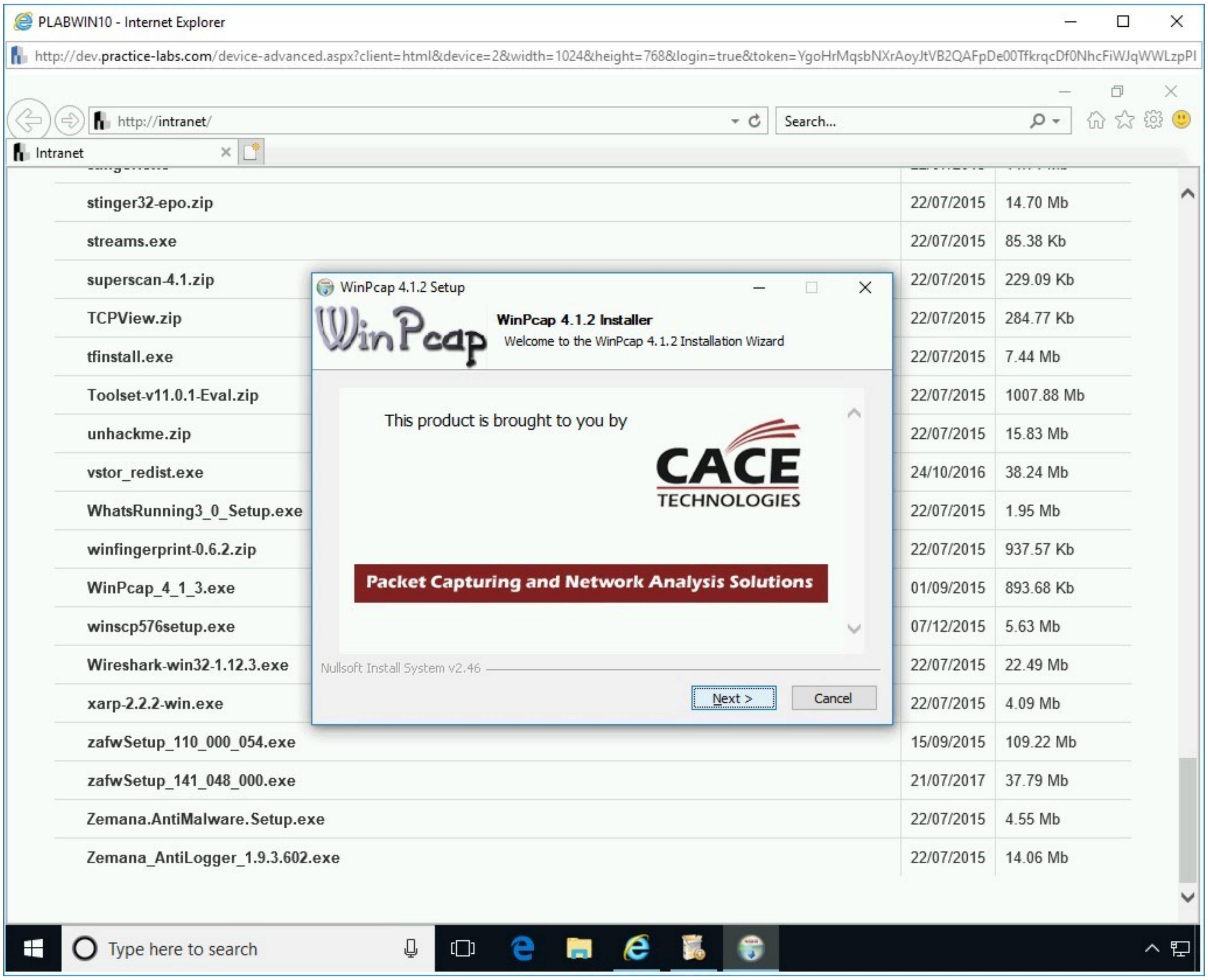
```
Output folder: C:\Program Files (x86)\XArp
Extract: pthreadVC2.dll... 100%
Extract: xarp.exe... 100%
Extract: WinPcap_4_1_2.exe
```

Figure 2.6 Screenshot of PLABWIN10: Showing the installation progress.

Step 7

Alert: The WinPcap 4.1.2 installation will be initiated ONLY if you have not installed WinPcap with any other tool. If WinPcap is found on the system, the XArp installation will proceed without Step 7 to Step 11. These steps will be skipped.

The **WinPcap 4.1.2 Setup** wizard is displayed. On the **WinPcap 4.1.2 Installer** page, click **Next**.

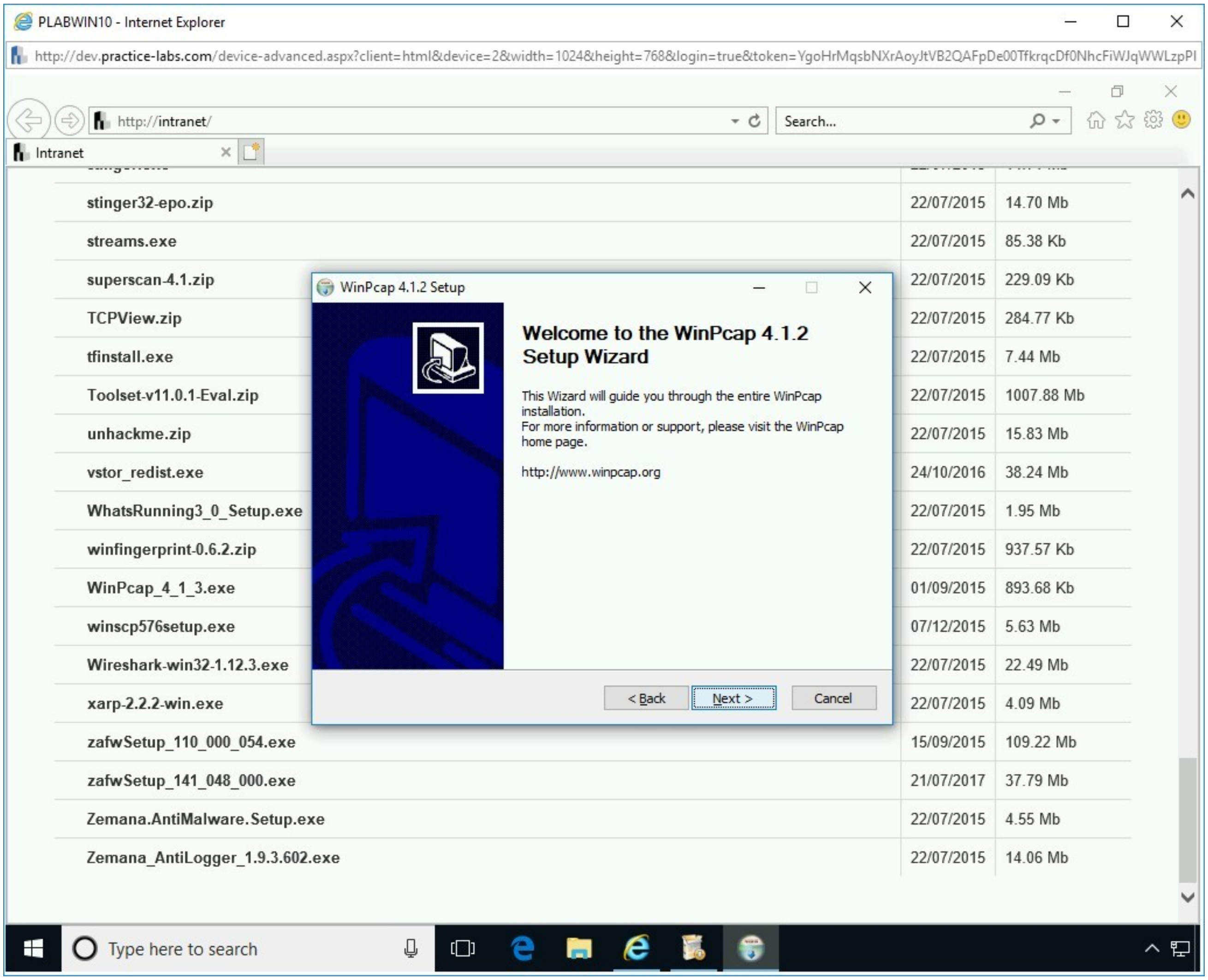

PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
WinPcap 4.1.2 Setup
WinPcap
WinPcap 4.1.2 Installer
Welcome to the WinPcap 4.1.2 Installation Wizard
This product is brought to you by
CACE TECHNOLOGIES
Packet Capturing and Network Analysis Solutions
Nullsoft Install System v2.46
Next >
Cancel
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

Figure 2.7 Screenshot of PLABWIN10: Clicking Next on the WinPcap wizard.

Step 8

On the **Welcome to the WinPcap 4.1.2 Setup Wizard** page, click **Next**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
WinPcap 4.1.2 Setup
< Back
Next >
Cancel
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

Welcome to the WinPcap 4.1.2 Setup Wizard

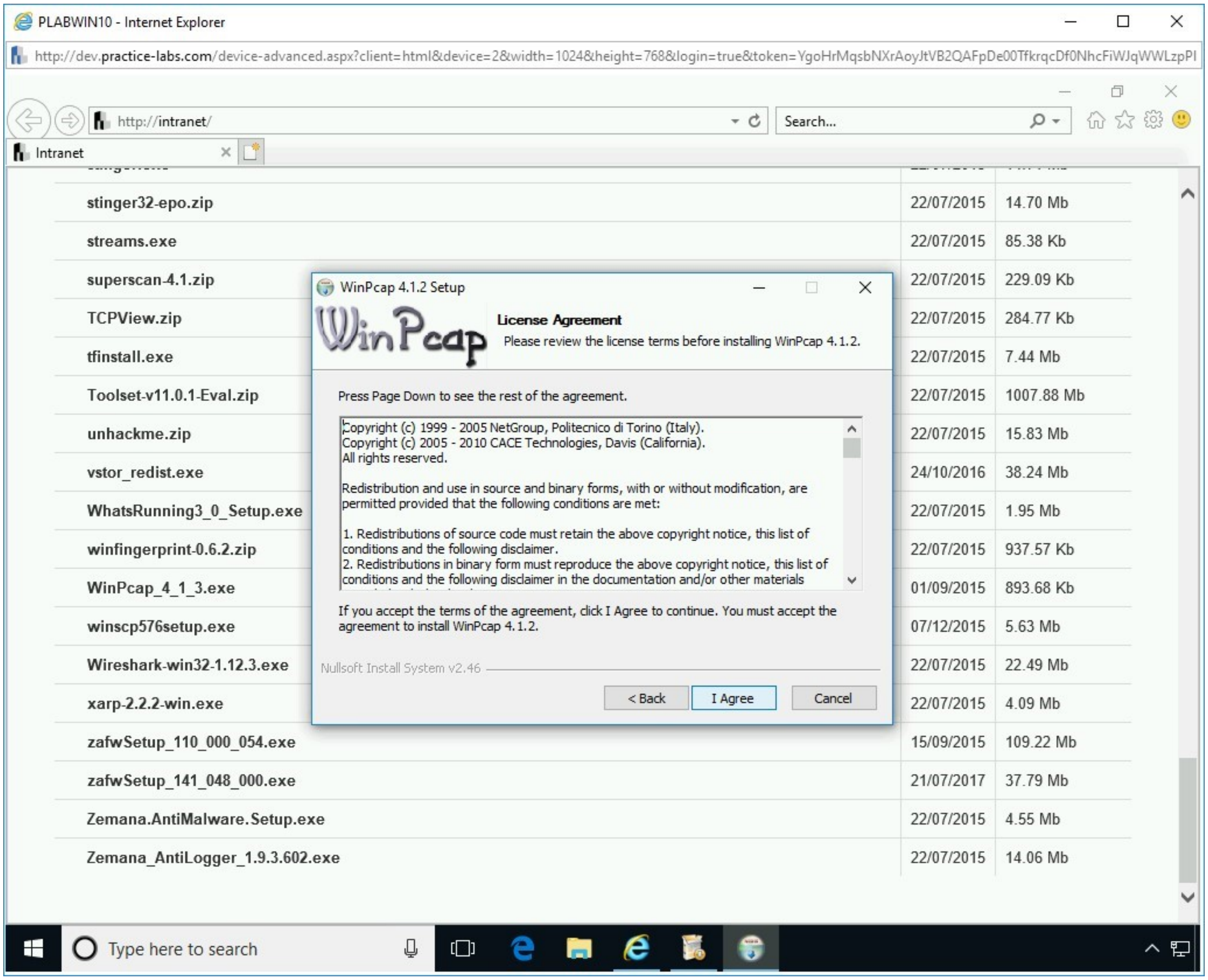
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.

http://www.winpcap.org

Figure 2.8 Screenshot of PLABWIN10: Clicking Next on the welcome page.

Step 9

On the **License Agreement** page, click **I Agree**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPl
http://intranet/
Search...
Intranet
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

WinPcap 4.1.2 Setup

License Agreement

Please review the license terms before installing WinPcap 4.1.2.

Press Page Down to see the rest of the agreement.

Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

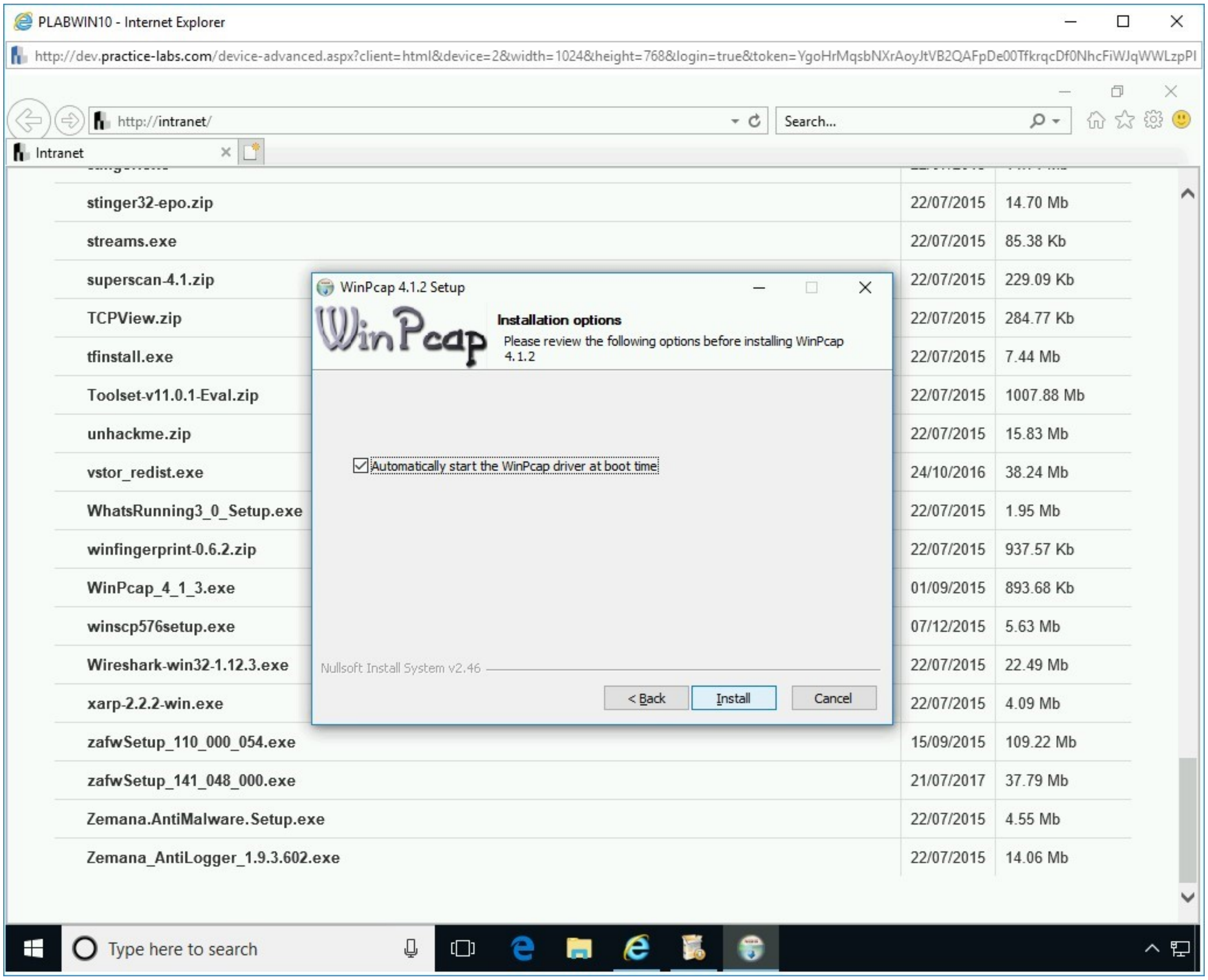
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.2.

Figure 2.9 Screenshot of PLABWIN10: Clicking I Agree on the License Agreement page.

Step 10

On the **Installation options** page, keep the default option selected and click **Install**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
WinPcap 4.1.2 Setup
WinPcap
< Back
Install
Cancel
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

Installation options

Please review the following options before installing WinPcap 4.1.2

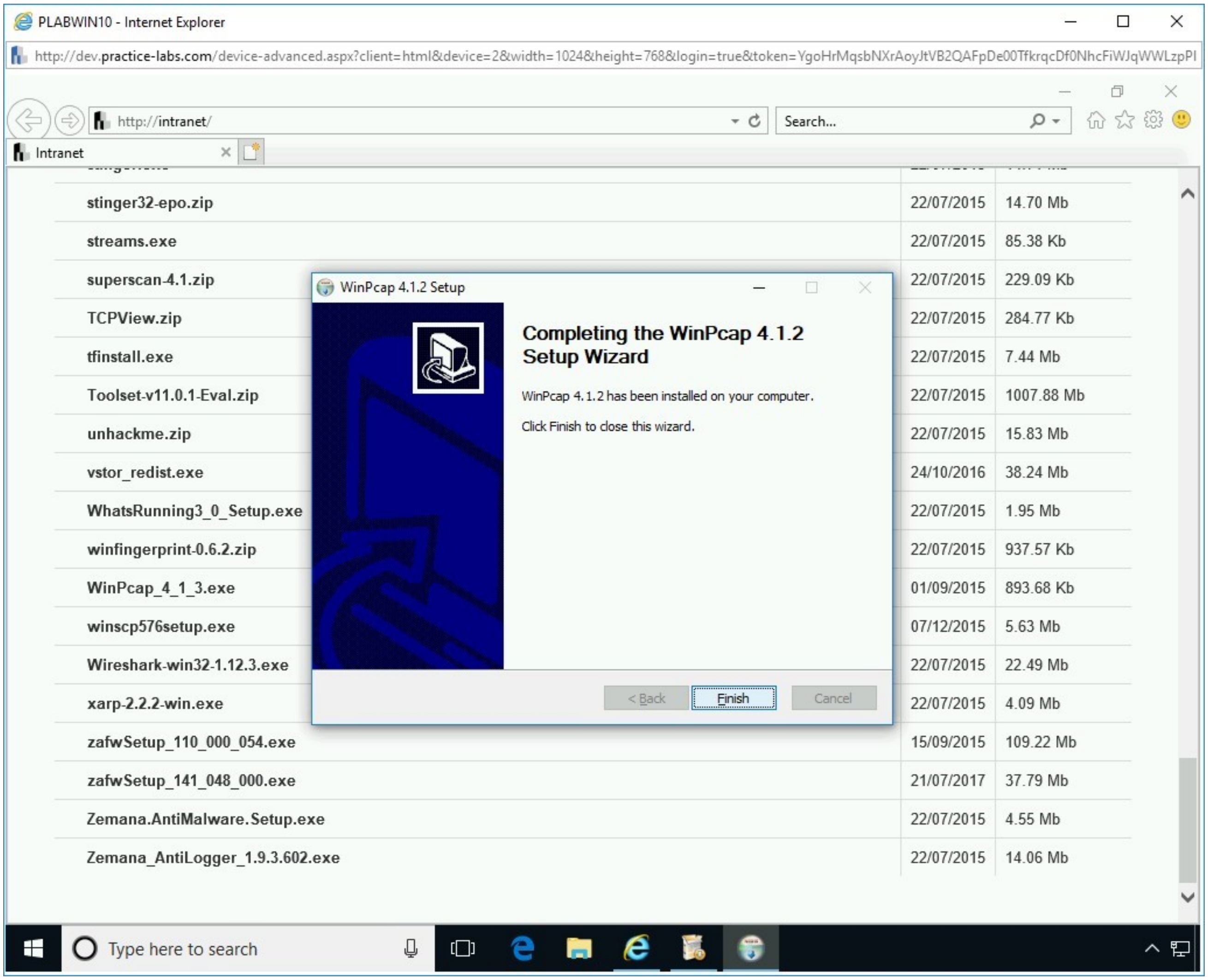
☑ Automatically start the WinPcap driver at boot time

Nullsoft Install System v2.46

Figure 2.10 Screenshot of PLABWIN10: Clicking Install on the Installation Options page.

Step 11

The installation completes quickly. On the **Completing the WinPcap 4.1.2 Setup Wizard** page, click **Finish**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
WinPcap 4.1.2 Setup
< Back
Finish
Cancel
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

Completing the WinPcap 4.1.2 Setup Wizard

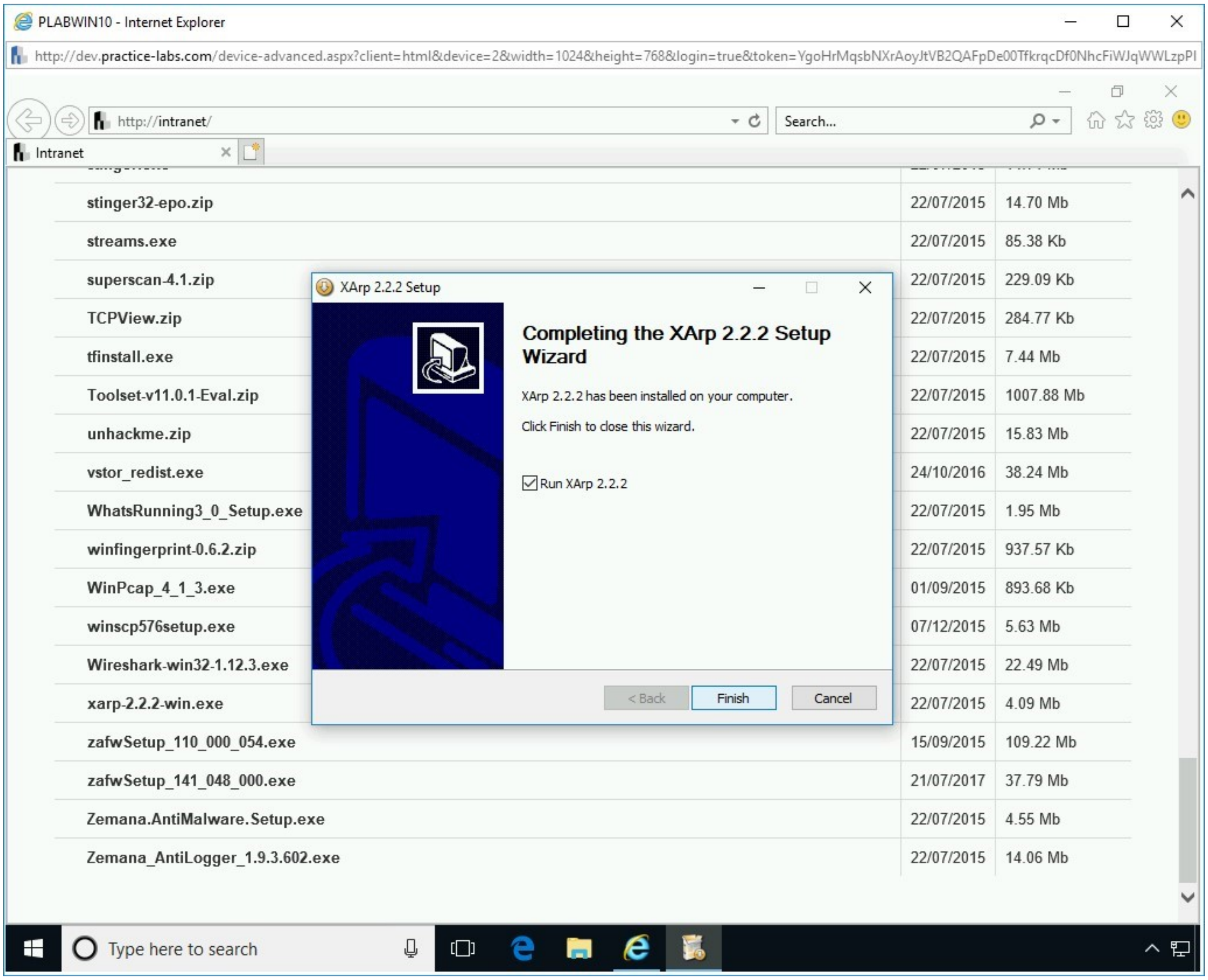
WinPcap 4.1.2 has been installed on your computer.

Click Finish to close this wizard.

Figure 2.11 Screenshot of PLABWIN10: Clicking Finish on the completion page.

Step 12

On the **Completing the XArp 2.2.2 Setup Wizard** page, keep the default option selected and click **Finish**.



PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
http://intranet/
Search...
Intranet
Type here to search

stinger32-epo.zip	22/07/2015	14.70 Mb
streams.exe	22/07/2015	85.38 Kb
superscan-4.1.zip	22/07/2015	229.09 Kb
TCPView.zip	22/07/2015	284.77 Kb
tfinstall.exe	22/07/2015	7.44 Mb
Toolset-v11.0.1-Eval.zip	22/07/2015	1007.88 Mb
unhackme.zip	22/07/2015	15.83 Mb
vstor_redist.exe	24/10/2016	38.24 Mb
WhatsRunning3_0_Setup.exe	22/07/2015	1.95 Mb
winfingerprint-0.6.2.zip	22/07/2015	937.57 Kb
WinPcap_4_1_3.exe	01/09/2015	893.68 Kb
winscp576setup.exe	07/12/2015	5.63 Mb
Wireshark-win32-1.12.3.exe	22/07/2015	22.49 Mb
xarp-2.2.2-win.exe	22/07/2015	4.09 Mb
zafwSetup_110_000_054.exe	15/09/2015	109.22 Mb
zafwSetup_141_048_000.exe	21/07/2017	37.79 Mb
Zemana.AntiMalware.Setup.exe	22/07/2015	4.55 Mb
Zemana_AntiLogger_1.9.3.602.exe	22/07/2015	14.06 Mb

XArp 2.2.2 Setup

Completing the XArp 2.2.2 Setup Wizard

XArp 2.2.2 has been installed on your computer.

Click Finish to close this wizard.

☑ Run XArp 2.2.2

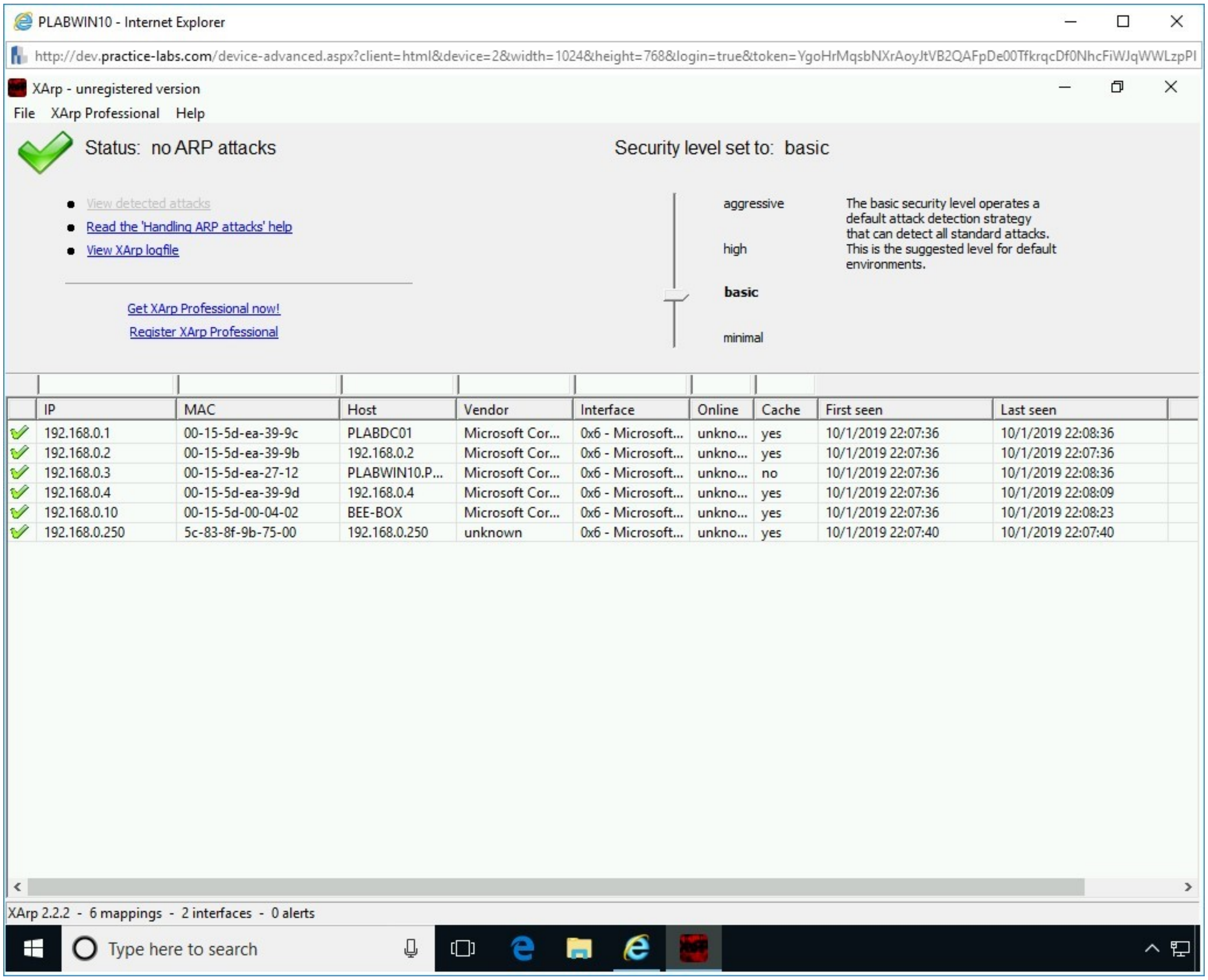
Figure 2.12 Screenshot of PLABWIN10: Clicking Finish on the completion page.

Step 13

Minimize **Internet Explorer**.

XArp automatically opens after installation.

Note that the default security level is set to **basic**.


PLABWIN10 - Internet Explorer
http://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=YgoHrMqsbNXrAoyJtVB2QAFpDe00TfkrqcDf0NhcFiWJqWWLzpPI
XArp - unregistered version
File
XArp Professional
Help
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal
Type here to search

Status: no ARP attacks

Security level set to: basic

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen
✓	192.168.0.1	00-15-5d-ea-39-9c	PLABDC01	Microsoft Cor...	0x6 - Microsoft...	unkno...	yes	10/1/2019 22:07:36	10/1/2019 22:08:36
✓	192.168.0.2	00-15-5d-ea-39-9b	192.168.0.2	Microsoft Cor...	0x6 - Microsoft...	unkno...	yes	10/1/2019 22:07:36	10/1/2019 22:07:36
✓	192.168.0.3	00-15-5d-ea-27-12	PLABWIN10.P...	Microsoft Cor...	0x6 - Microsoft...	unkno...	no	10/1/2019 22:07:36	10/1/2019 22:08:36
✓	192.168.0.4	00-15-5d-ea-39-9d	192.168.0.4	Microsoft Cor...	0x6 - Microsoft...	unkno...	yes	10/1/2019 22:07:36	10/1/2019 22:08:09
✓	192.168.0.10	00-15-5d-00-04-02	BEE-BOX	Microsoft Cor...	0x6 - Microsoft...	unkno...	yes	10/1/2019 22:07:36	10/1/2019 22:08:23
✓	192.168.0.250	5c-83-8f-9b-75-00	192.168.0.250	unknown	0x6 - Microsoft...	unkno...	yes	10/1/2019 22:07:40	10/1/2019 22:07:40

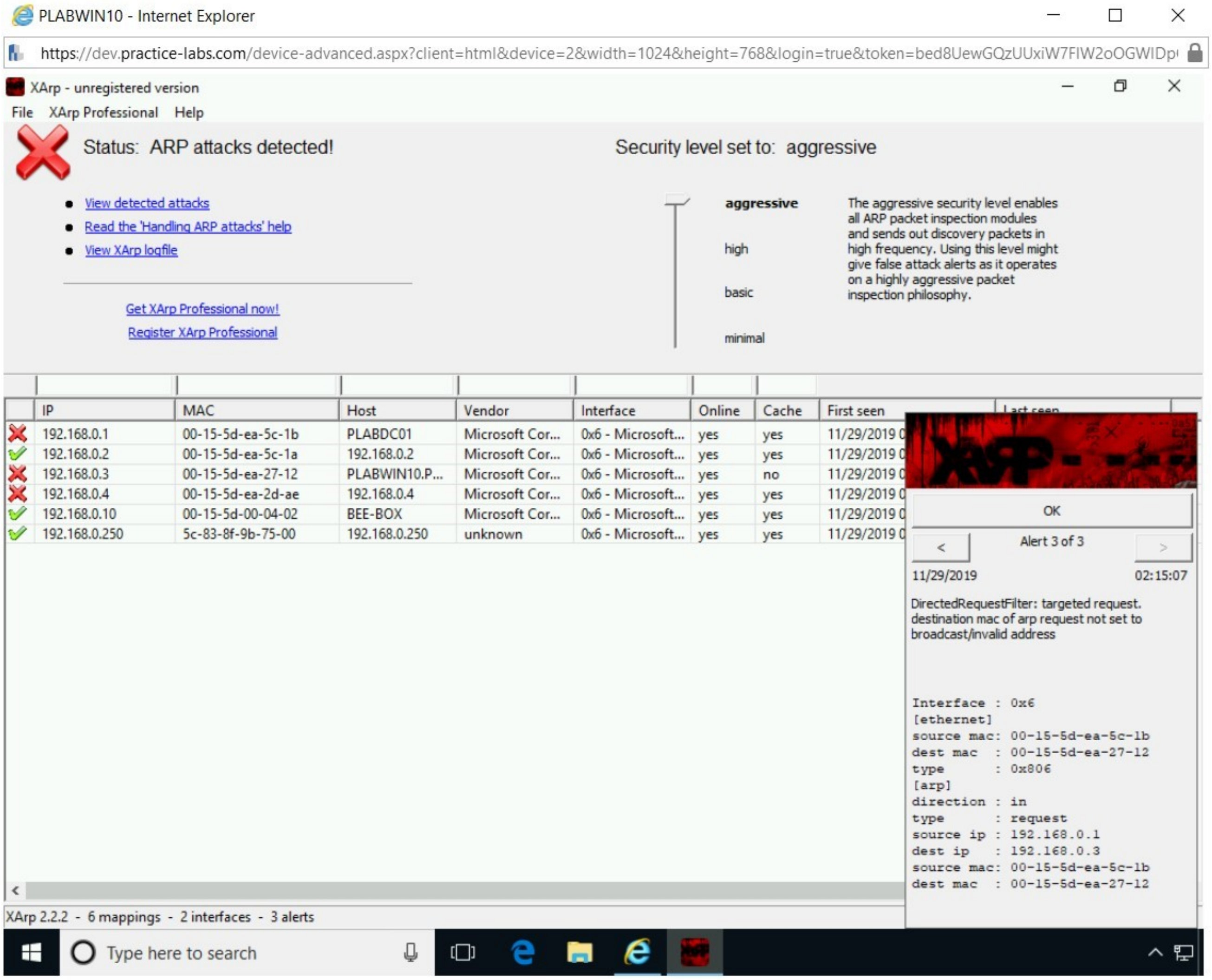
XArp 2.2.2 - 6 mappings - 2 interfaces - 0 alerts

Figure 2.13 Screenshot of PLABWIN10: Showing XArp window with the basic security level.

Step 14

Move the slider to **aggressive**. Notice that there are ARP attacks on the network are detected. Click **OK** in the right-hand pane.

> ***Note***: *It may take a few seconds for XArp to detect an attack.*



PLABWIN10 - Internet Explorer

https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bed8UewGQzUUxiW7FIW2oOGWIDp

XArp - unregistered version

Status: ARP attacks detected!

Security level set to: aggressive

- View detected attacks
- Read the 'Handling ARP attacks' help
- View XArp logfile

Get XArp Professional now!
Register XArp Professional

The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
✗	192.168.0.1	00-15-5d-ea-5c-1b	PLABDC01	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 0
✓	192.168.0.2	00-15-5d-ea-5c-1a	192.168.0.2	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 0
✗	192.168.0.3	00-15-5d-ea-27-12	PLABWIN10.P...	Microsoft Cor...	0x6 - Microsoft...	yes	no	11/29/2019 0
✗	192.168.0.4	00-15-5d-ea-2d-ae	192.168.0.4	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 0
✓	192.168.0.10	00-15-5d-00-04-02	BEE-BOX	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 0
✓	192.168.0.250	5c-83-8f-9b-75-00	192.168.0.250	unknown	0x6 - Microsoft...	yes	yes	11/29/2019 0

11/29/2019 02:15:07

DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/invalid address

```
Interface : 0x6
[ethernet]
source mac: 00-15-5d-ea-5c-1b
dest mac  : 00-15-5d-ea-27-12
type      : 0x806
[arp]
direction : in
type      : request
source ip : 192.168.0.1
dest ip   : 192.168.0.3
source mac: 00-15-5d-ea-5c-1b
dest mac  : 00-15-5d-ea-27-12
```

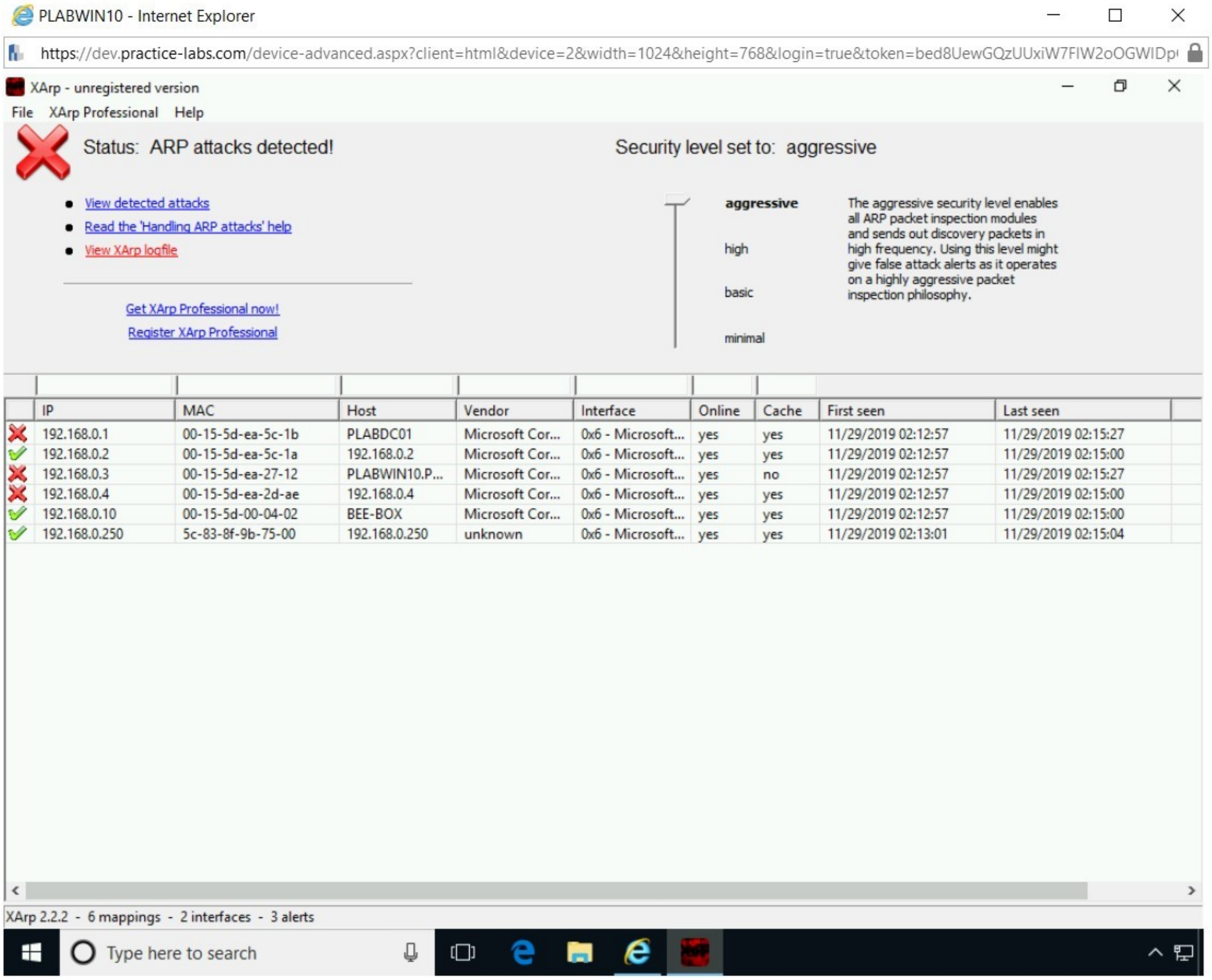
XArp 2.2.2 - 6 mappings - 2 interfaces - 3 alerts

Figure 2.14 Screenshot of PLABWIN10: Showing XArp window with the high security level and arp attack detected.

Step 15

You can also view the detailed log.

Click **View XArp logfile**.



PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bed8UewGQzUUxiW7FIW2oOGWIDp
XArp - unregistered version
File XArp Professional Help

Status: ARP attacks detected!

Security level set to: aggressive

- View detected attacks
- Read the 'Handling ARP attacks' help
- View XArp logfile

Get XArp Professional now!
Register XArp Professional
aggressive
high
basic
minimal

The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

	IP	MAC	Host	Vendor	Interface	Online	Cache	First seen	Last seen
✗	192.168.0.1	00-15-5d-ea-5c-1b	PLABDC01	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 02:12:57	11/29/2019 02:15:27
✓	192.168.0.2	00-15-5d-ea-5c-1a	192.168.0.2	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 02:12:57	11/29/2019 02:15:00
✗	192.168.0.3	00-15-5d-ea-27-12	PLABWIN10.P...	Microsoft Cor...	0x6 - Microsoft...	yes	no	11/29/2019 02:12:57	11/29/2019 02:15:27
✗	192.168.0.4	00-15-5d-ea-2d-ae	192.168.0.4	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 02:12:57	11/29/2019 02:15:00
✓	192.168.0.10	00-15-5d-00-04-02	BEE-BOX	Microsoft Cor...	0x6 - Microsoft...	yes	yes	11/29/2019 02:12:57	11/29/2019 02:15:00
✓	192.168.0.250	5c-83-8f-9b-75-00	192.168.0.250	unknown	0x6 - Microsoft...	yes	yes	11/29/2019 02:13:01	11/29/2019 02:15:04

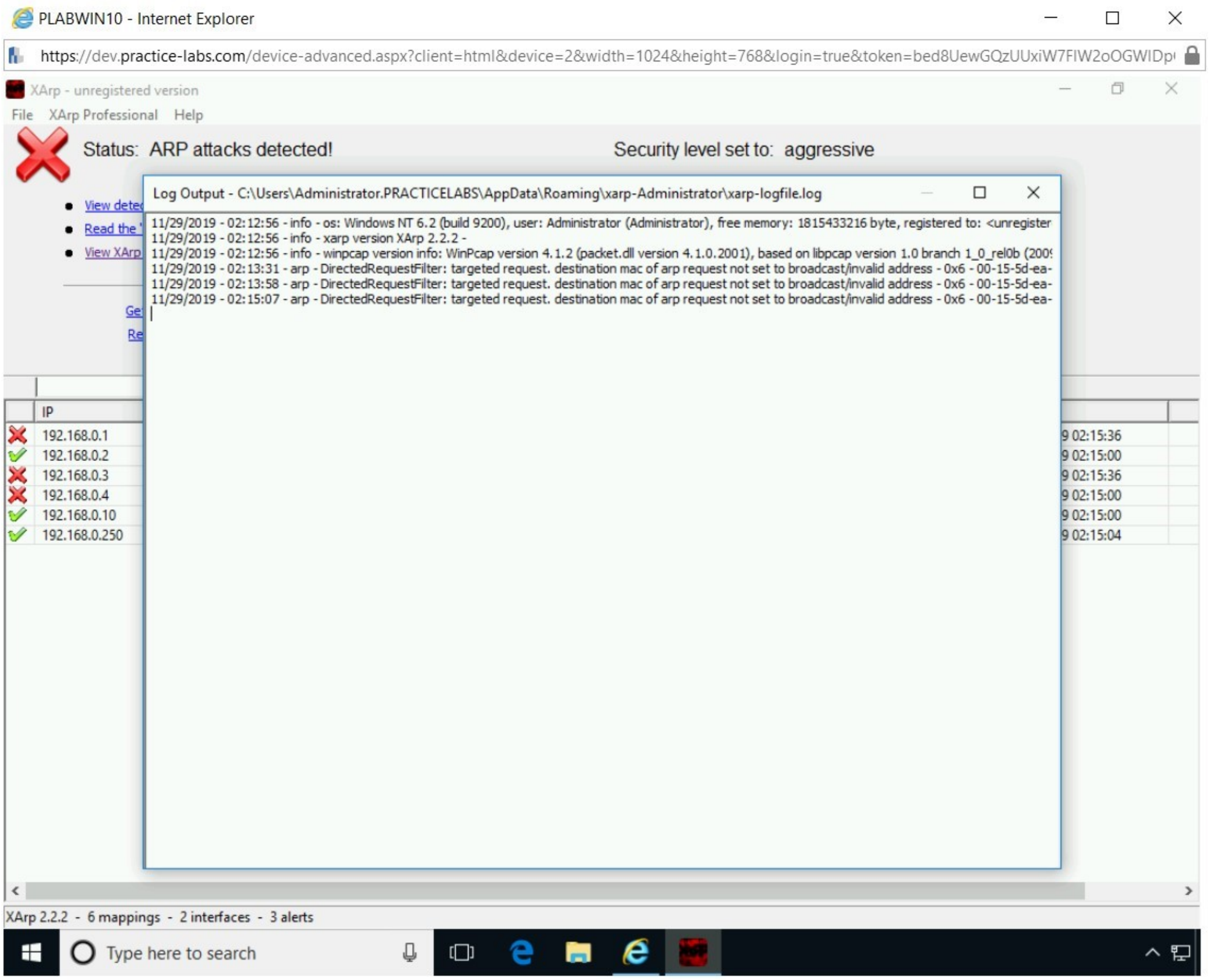
XArp 2.2.2 - 6 mappings - 2 interfaces - 3 alerts

Figure 2.15 Screenshot of PLABWIN10: Clicking the View XArp logfile link.

Step 16

The **Log Output** file is displayed.

A detailed list of events is entered into this log file.


PLABWIN10 - Internet Explorer
https://dev.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=bed8UewGQzUUxiW7FIW2oOGWIDp
XArp - unregistered version
File
XArp Professional
Help
View detec
Read the '
View XArp
Ge
Re
Type here to search

Status: ARP attacks detected!

Security level set to: aggressive

Log Output - C:\Users\Administrator.PRACTICELABS\AppData\Roaming\xarp-Administrator\xarp-logfile.log

```
11/29/2019 - 02:12:56 - info - os: Windows NT 6.2 (build 9200), user: Administrator (Administrator), free memory: 1815433216 byte, registered to: <unregister
11/29/2019 - 02:12:56 - info - xarp version XArp 2.2.2 -
11/29/2019 - 02:12:56 - info - winpcap version info: WinPcap version 4.1.2 (packet.dll version 4.1.0.2001), based on libpcap version 1.0 branch 1_0_rel0b (200
11/29/2019 - 02:13:31 - arp - DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/invalid address - 0x6 - 00-15-5d-ea-
11/29/2019 - 02:13:58 - arp - DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/invalid address - 0x6 - 00-15-5d-ea-
11/29/2019 - 02:15:07 - arp - DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/invalid address - 0x6 - 00-15-5d-ea-
```

	IP	
✗	192.168.0.1	9 02:15:36
✓	192.168.0.2	9 02:15:00
✗	192.168.0.3	9 02:15:36
✗	192.168.0.4	9 02:15:00
✓	192.168.0.10	9 02:15:00
✓	192.168.0.250	9 02:15:04

XArp 2.2.2 - 6 mappings - 2 interfaces - 3 alerts

Figure 2.16 Screenshot of PLABWIN10: Showing the log file and closing XArp.

Close **XArp**.

Review

Well done, you have completed the **Sniffing** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Sniffing Techniques and Analysis

- Exercise 2 - Sniffing Prevention Techniques

You should now be able to:

- Use MAC Address Changer: Change MAC Address
- Use SMAC 2.0
- Install Wireshark
- Use Wireshark
- Use Sniff-O-Matic
- Use XArp utility

Feedback

Shutdown all virtual machines used in this lab. Alternatively, you can log out of the lab platform.