**Introduction to Network Traffic Analysis with Wireshark**

**Directions for Kali – Hardware on Raspberry Pi**

**Dr. Shannon Beck, Updated 12/30/21**

**Introduction**

**Lab Description:** In this lab, you will learn some basics about networks using Wireshark. Wireshark is a very useful tool for network forensics–viewing and storing (capturing) networking traffic. Wireshark is software that is called a packet analyzer. It enables you to view pieces of data (called packets) in real-time as they go in and out of a system. You can save these packets as packet capture (pcap or cap) files. In this lab, you will capture live network traffic in real-time and analyze previously captured packet files.

**Objectives**

* Use Wireshark and gain familiarity with the software tool
* Perform network packet capture through Wireshark
* Inspect packet capture (pcap) files in Wireshark
* Lean more about DNS, MAC addresses and WLANs

**Lab Environment**: Kali Linux

**Setting Up the Environment**

1. Log on to your Kali Linux virtual machine using the username kali and the password kali
2. Navigate to “09 ->Sniffing & Spoofing” -> wireshark
3. When prompted to run Wireshark with root permissions, enter the password **kali** and press Enter

Figure : Starting Wireshark through GUI

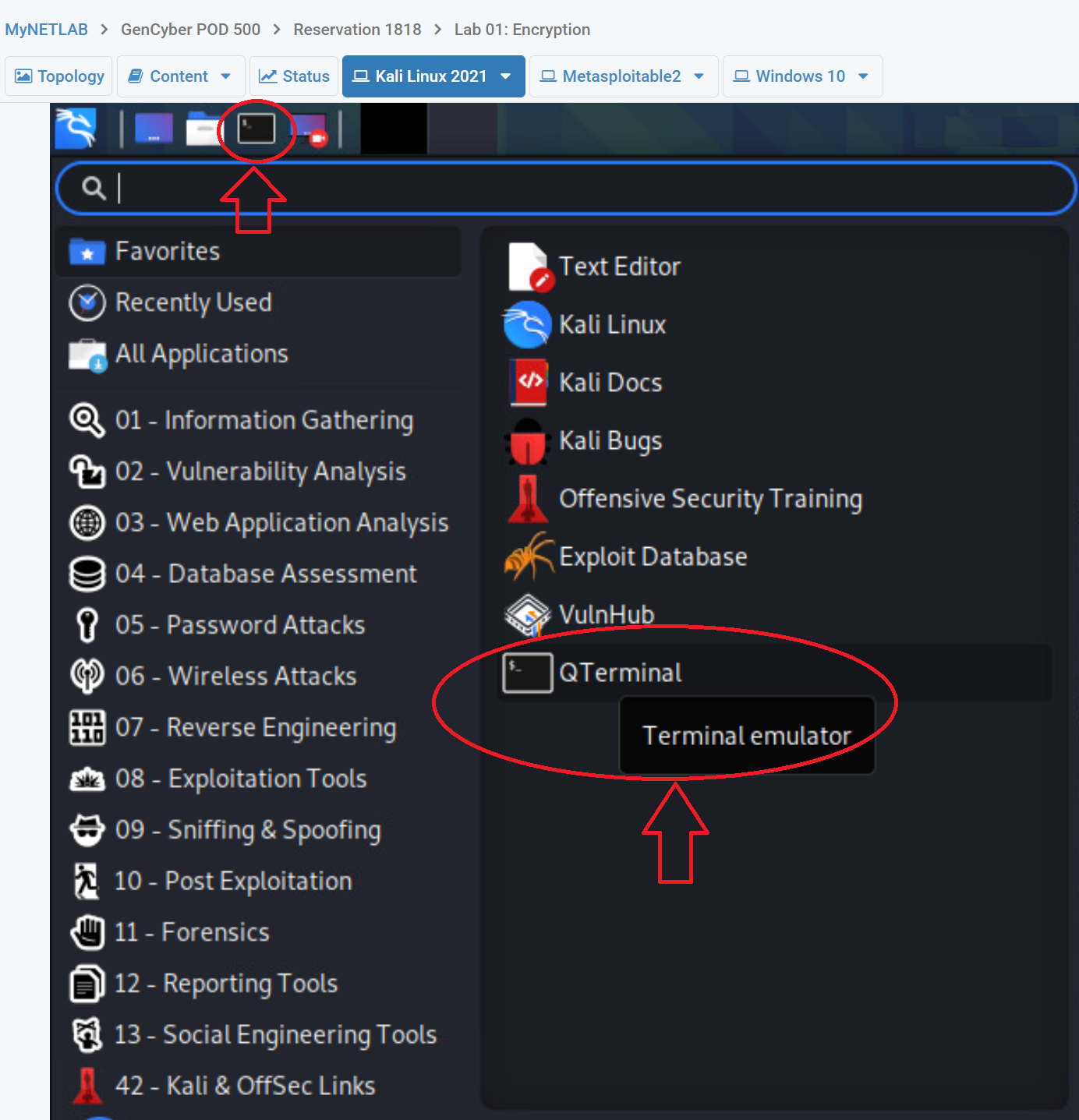
*Alternative*:

Figure : Starting QTerminal

**Open up a terminal** or command-line interface (CLI). Referred to as the QTerminal in the Application menu, or you can click on the black computer screen terminal icon to launch the terminal window. Launch Wireshark.

From the terminal window type sudo wireshark

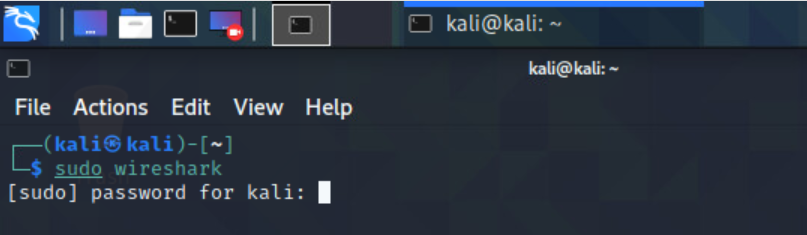


Figure : Starting Wireshark from CLI

When prompted to run Wireshark with root permissions, enter the password **kali** and press Enter.

If successful, Wireshark should open. Note: It may be necessary to launch this through the terminal window and not the menu system. This ensures that Wireshark opens with the needed administrative permission (using the sudo command) so that you can capture traffic.

If Wireshark does not start, open a QTerminal and type the sudo wireshark and enter the “kali” password.

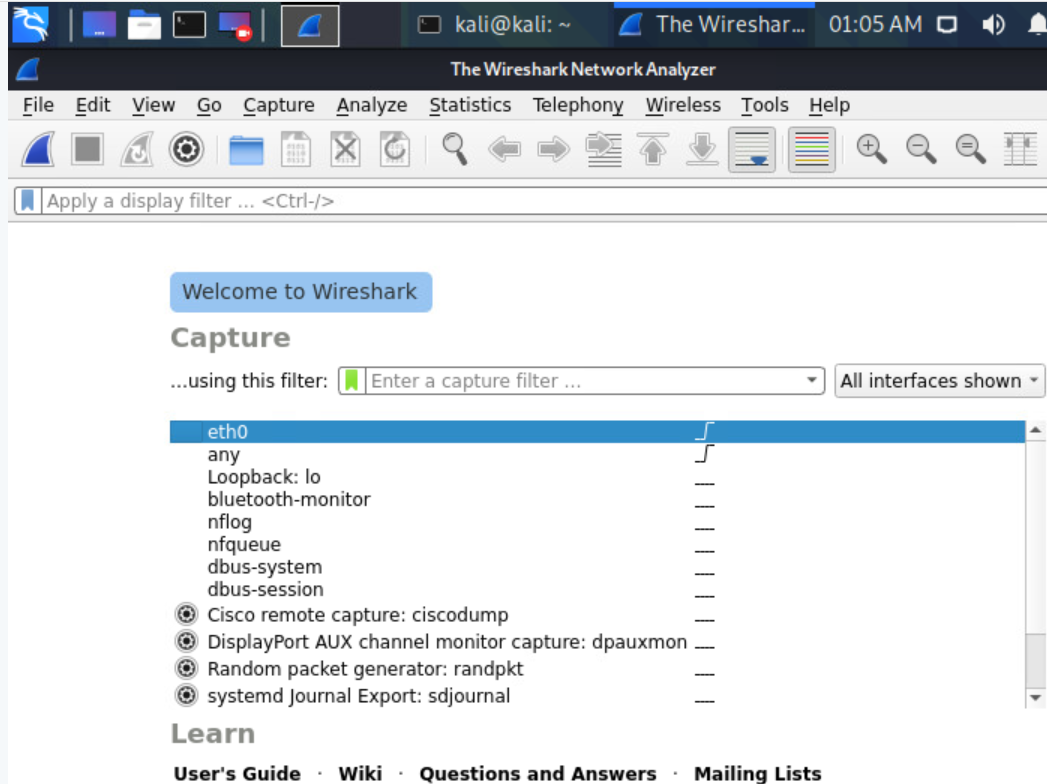


Figure : Wireshark interface when first started

Wireshark is a powerful analysis tool that allows you to capture network and device packets and analyze them too.

A packet is a fragment of data that is sent over a network from one machine to another. This data usually includes a *source port*, *source IP* *address*, *destination port*, *destination IP*, and other data that we will see in this lab.

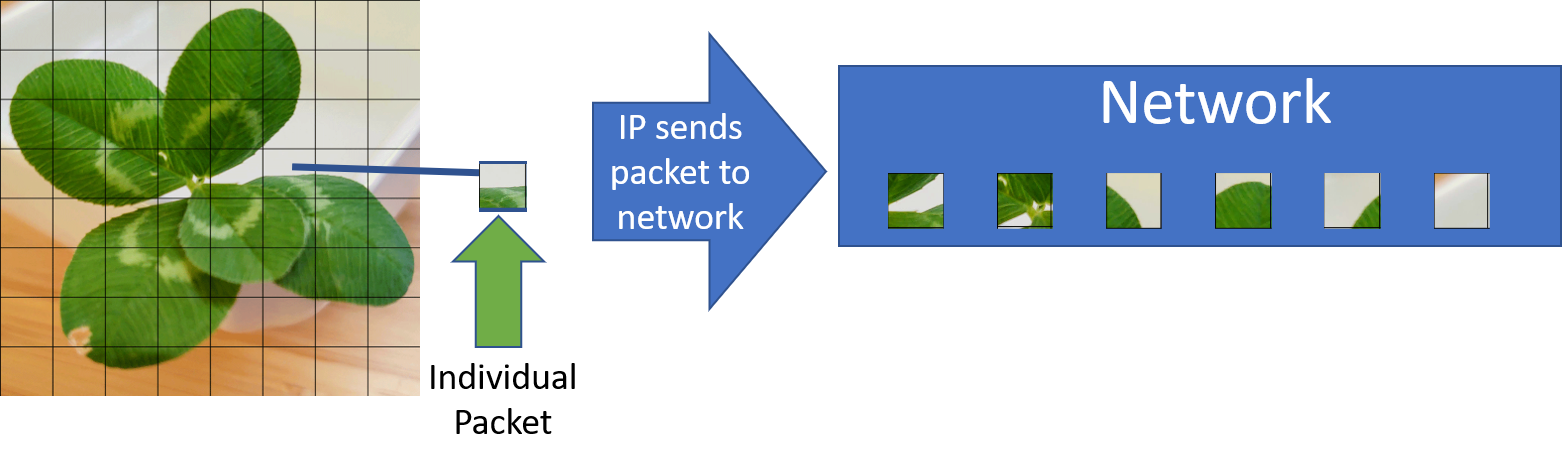


Figure : Concept of a packet sent across a network

Let’s explore the Wireshark application interface (not running any commands yet).

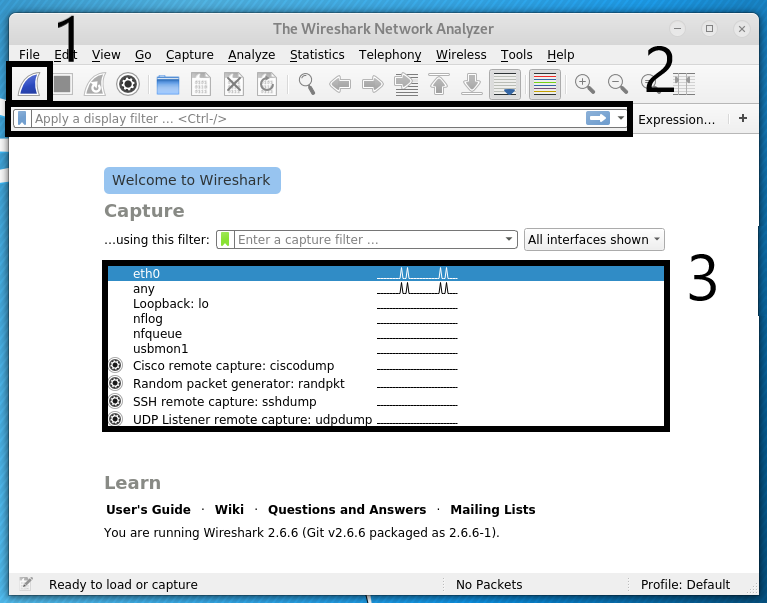


Figure : Wireshark - annotated interface upon startup

From the above image, we highlight several important Wireshark features through the annotations by the three numbered boxes:

1. **Start Capturing Packets:** This is the button to start a live packet capture. This will capture network traffic going in and out of your system in real-time.
2. **Filter String Field:** This field allows the user to apply filters to the traffic captured. Configure the filters based on your needs:
   * Text in the body of the packet
   * IP address (10.0.0.5)
   * Protocol (i.e. TCP)
   * Port (i.e. 80, 443)

Filtering is vital when searching through large amounts of data.

1. **Live Packet Devices:** This is a list of the network interfaces from which we can capture traffic. This can be an ethernet port or a wireless (wi-fi) card.

Once Wireshark starts capturing network traffic or opens a file, the screen will change.

Looking at Figure 7, we point out a few more important Wireshark features:

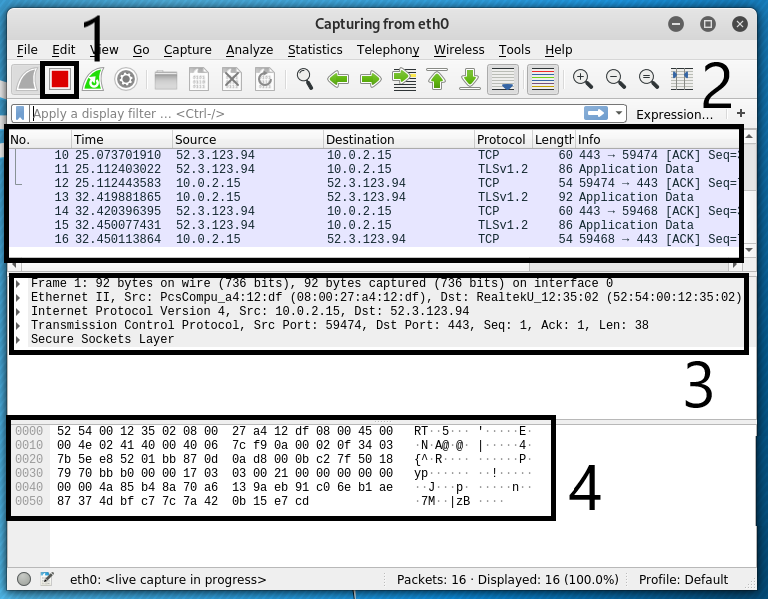


Figure : The three main inspection fames from a capture in Wireshark

1. **Stop Capture Button:** This button stops the current capture if you are collecting live network traffic. Once you click this, you can analyze the data and have the option to save it as a .pcap file (a file containing captured packet data) for further analysis or exporting.
2. **Packet List Pane:** This displays the captured data packets. It shows the Source IP, Destination IP, Protocol, and more information about each packet.
3. **Packet Details Pane:** After selecting a packet, this pane displays the packet’s data structure contained within the selected packet from the Packet List Pane (in Box #2). In the details pane, you can clearly see the Layer-1 through Layer-3 TCP/IP stack of encapsulated data structures. From the top, the Layer-1 frame and Ethernet data, wrapped in a Layer-2 IP datagram wrapped in a Layer-3 TCP transport session or connection.
4. **Packet Bytes Pane:** This displays the raw data of the highlighted packet (in Box #2) in its most basic or “canonical” hexadecimal + ASCII formats — the lowest level, most basic, binary data, represented in both hex (machine) and ASCII (human) readable formats side-by-side.

Now that we understand the basics using Wireshark to capture data, let’s look at a few pcap files, interpret the data in them, and see what we can learn!

### Task 1: Analyzing SQL Slammer Work pcap file

You will look at .pcap (pronounced “p cap”) files for analysis.

The first two files are from the Wireshark website. These samples are available on the Wireshark Wiki page at <https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures>.

* Under heading of [Viruses and worms](https://wiki.wireshark.org/SampleCaptures#Viruses_and_worms): [slammer.pcap](https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=slammer.pcap)
* Under heading of [General / Unsorted](https://wiki.wireshark.org/SampleCaptures#General_.2F_Unsorted): [dns.cap](https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=get&target=dns.cap)

The third file will take a look at some wireless (Wi-Fi) access points.

* Fake\_Access\_Point\_Beacons.pcap

The packet capture files are stored in the “Common -> Wireshark” folder on the Desktop.

1. From your running Wireshark program, be sure you have stopped collection (no need to save it

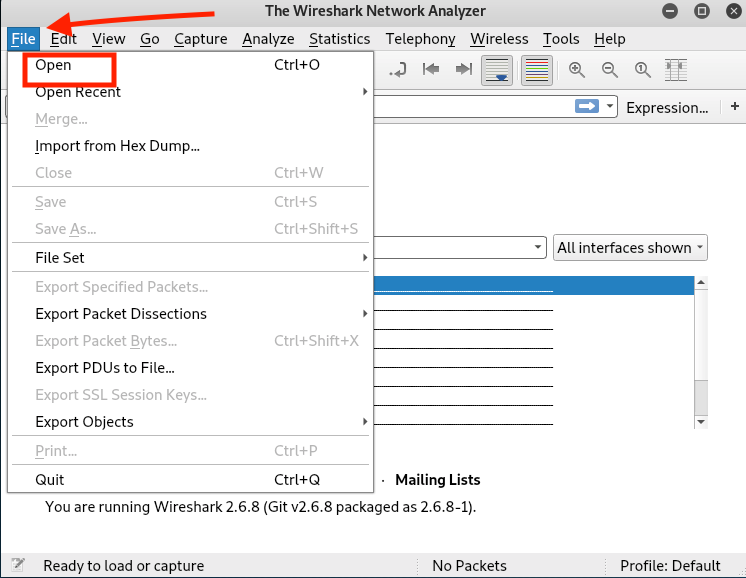


Figure : Opening a p(cap) file for analysis

Open the slammer.pcap file. To open it, click on the File menu, then click Open. Navigate to /home> kali> Desktop> Common> Wireshark.

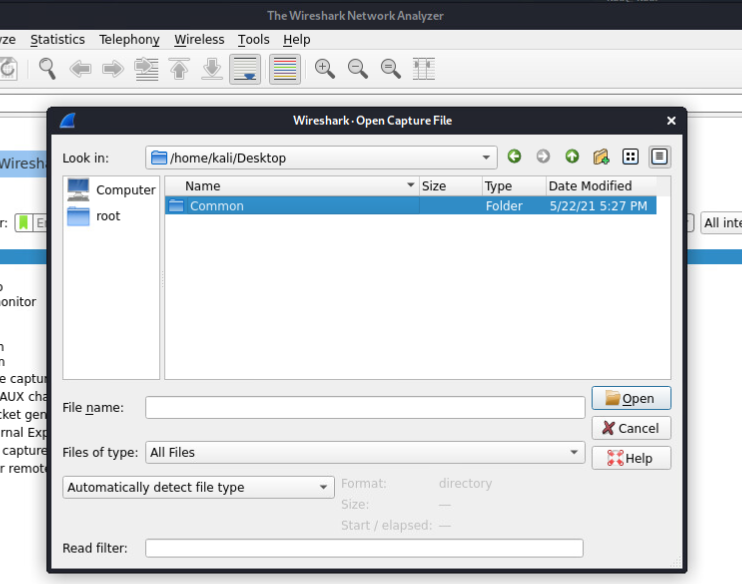
Select **slammer.pcap** and click on Open. This packet capture contains a single packet. The [SQL Slammer worm](https://en.wikipedia.org/wiki/SQL_Slammer) infected hosts through a single packet (!) and spread rapidly.

Figure : Navigating the Desktop>Common>Wireshark folders

1. Looking at the top packet in the Packet List Pane in the figure below, let’s see what information we can gather

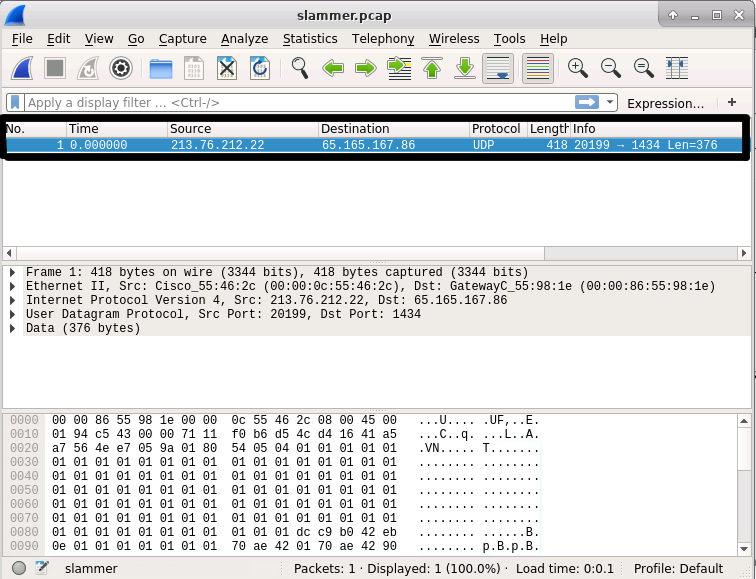


Figure : Inspecting the single packet from the slammer.pcap file

If you view the top window, this pane lists all of the packets in the capture (in this case, a single packet), as well as other basic information about the packets. The table below explains what each field means.

|  |  |
| --- | --- |
| **Field Name** | **Description** |
| No. | The packet number; this goes incrementally in order by which packets reach the machine or leave the machine first. |
| Time | This is the time from the first packet capture to the selected one; if it is the first packet, the time is 0.0. |
| Source | The IP address of the machine the packet originated from. The sender’s address. |
| Destination | The IP address of the intended recipient of the packet. The receiver’s address. |
| Protocol | The networking protocol used to send this packet. In Wireshark, if we desire we can filter captured data based on specific protocols. Specifically, this data is Network Layer traffic and we can see this packet is using the User Datagram Protocol (UDP) protocol as opposed to TCP traffic. |
| Length | The data length/size of the packet. |
| Info | Details about the packet; sometimes helpful. |

The Packet Details pane allows you to analyze the packet highlighted in the Packet List Pane.

Use the Packet Details Pane to analyze the details of the **slammer.pcap** file to answer the questions below.

#### Question 1: What is the *DESTINATION* *port* of the packet in question? Hint the DESTINATION IP address IS 65.165.167.86. The SQL Server Browser service listens on this port for incoming connections.

#### Question 2: Name the protocol used to spread the SQL Slammer Worm in this packet.

#### Extension activity: Explore the web to learn more about the slammer worm. What type of applications did it impact and target? What year did it first appear?

### Task 2: Analyzing DNS Packets

*A brief overview of DNS*

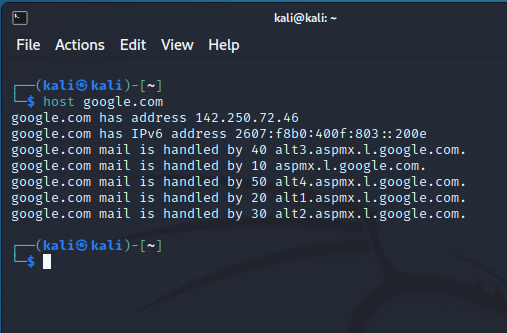
Phonebook with the label "DNS" and a series of Domain names and corresponding IP addresses.
The first line is google.com <--> 173.194.77.104. 

Image from https://tibbbz.medium.com/pi-hole-dns-for-dummies-5763b65ee527
When you enter “google.com” into the web browser, this name has to be translated into a (destination) IP address. This allows the TCP/IP protocol to connect your web browser to a Google server and serve the content that the Google server provides.

This text name translation from google.com to an IP address is completed through the Domain Name System (DNS). Think of having a phonebook lookup for webpages. The text URL is the “name” and the IP address is like the phone number in a phonebook.

You can manually look up the DNS record to translate google.com into its IP address by typing the DNS lookup command at the CLI or terminal. Open up QTerminal Emulator if you have not already and type:

host google.com



This will resolve (translate) the domain google.com to one or more IPv4 addresses (called A records), IPv6 addresses (called AAAA records), and also provide the known email servers that handle email traffic for that domain (called mail exchange (MX) records). This type of DNS resolution happens every time you visit a website, click on a link, or send an email.

To understand how the Domain Name System (DNS) works, we will explore the dns.cap packet capture file.

1. Open the dns.cap file by selecting Wireshark’s **File / Open or Ctrl+O**. It is in the same /home/kali/Desktop/Common/Wireshark directory

Right away, you’ll notice this DNS capture (dns.cap) has many more packets than the last one. See the figure below. In the Packet List pane, select the 10th packet (No. 10) and explore some of the content in the Packet Details panel.

*Hint: you can resize the window to make it easier to view the packet data.*

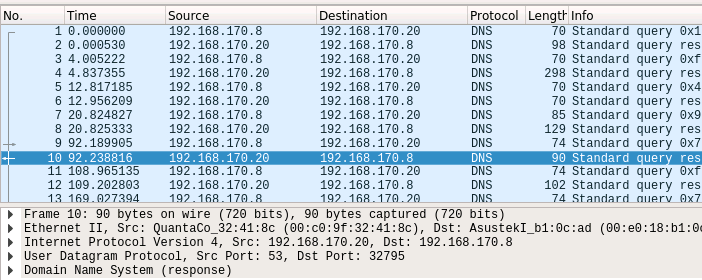
1. In the Packet Details pane, we can examine much more of the packet’s internal details. Let’s examine the DNS information for packet no. 10. See the figure below

Figure : dns.cap file opened in Wireshark

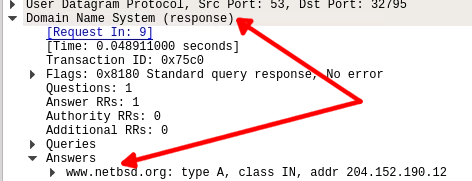


Figure : Packet Details Pane with expanded entries

Expand the **Domain Name System (response)** by clicking on the arrow to the left of the text.

1. Expand the **Answers** entry and you should see an IP response for the domain [www.netbsd.org](http://www.netbsd.org/). This means that a DNS query was made for the domain [www.netbsd.org](http://www.netbsd.org/) and the IP address of the website was successfully retrieved at 204.152.90.12

#### Question 3: In Packet No. 5, what URL was queried for its DNS information?

#### Hint: look under “Domain Name System (response)” and expand the “Queries” tab.

Note: the DNS response is in packet 6 (helpfully noted by Wireshark).

#### Question 4: In Packet No. 5 (and all of these DNS packets), what protocol is used?

#### Question 5: What is the IP address of the Domain Name Server (i.e. the source computer that provides the responses to the queries)? This is the source IP address of the packets that have the DNS responses (answers) such as in Packets 6 and 8.

### Task 3: Analyzing Wireless Packets

Wireless networks have become very common in providing internet connectivity. With this connectivity, come attacks from physically nearby sources. Home wireless networks and large corporate networks are all vulnerable to these attacks. Hackers employ tools to search for unsecured networks in order to steal internet access or to break into networks. In fact, Kali has several tools that can assist in setting up this type of attack.

Attackers might accomplish this by going to common hangouts such as restaurants, hotels, or coffee shops that offer free Wi-Fi. Through the use of wireless sniffing tools or even a regular wi-fi interface, unsecured networks are discovered. Attackers can also use hot-spots to set up rouge access points (APs) to fool people into connecting to these access points. The objective of this task is to perform network traffic packet analysis to identify rouge APs.

**Find the rouge access point**

In this exercise, you will determine if any rouge APs have been deployed in the network.

1. In Wireshark, select **File** then **Open**
2. In the Desktop > Common > Wireshark directory, select the **Fake\_Access\_Point\_Beacon.pcap** file and click **Open**. Wireshark will load this file for you to analyze.

Figure : Opening Fake\_Access\_Point\_Beacons.pcap

1. Once the file has loaded, you should see the screen below

Screenshot of Fake Access Point Beacons pcap file
Source: Wireshark, Kali Linux VM



Figure : Wireshark Fake\_Access\_Point\_Beacons.pcap opened in Wireshark

1. Click on one of the lines shown in the top frame.
2. Go to the middle frame and click the arrow next to the IEEE 802.11 Beacon frame

Location of IEEE 802.11 Beacon Frame in Fake Access Point Beacons pcap file
Source: Wireshark, Kali Linux VM


Figure : Navigating in Wireshark, inspecting a Beacon Frame

1. Look at the **source address** and **BSSID** (stands for Basic Service Set ID)

Location of IBSS Id in Fake Access Point Beacons pcap file
Source: Wireshark, Kali Linux VM


Figure : Locating and inspecting the BSS id in Wireshark

1. The first part is the vendor name. The second part in parenthesis is the full MAC (hardware) address. This is way to identify a specific piece of hardware or AP.
2. Compare the **BSSID**, **vendor name** and **MAC address** against the whitelist.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Vendor | Mac Address | SSID | Channel | BSSID |
| AP | Netgear | 00:1f:33:45:56:56 | \*\*\*\*\*\*\*\*\*\*\*\* | 6 | Netgear\_45:56:56 |
| AP | Cisco-Li | 0c:68:03:d6:88:78 | Test | 48 | Cisco-Li\_d6:88:78 |
| AP | Netgear | 00:1f:33:45:90:90 | BBBBBBBBBBBB | 6 | Netgear\_45:90:90 |

**Approved whitelist of good/allowed network devices**

**BSS Id: Netgear\_45:56:56 (00:1f:33:45:56:56)**

1. Click on **Wireless > WLAN Traffic**

WLAN traffic of Fake Access Point Beacons pcap file
Source: Wireshark, Kali Linux VM



Figure : Taking a deeper look at the wi-fi traffic

1. Look at the **BSSID, Channel** and **SSIDs** listed WLAN traffic of Fake Access Point Beacons pcap file
   Source: Wireshark, Kali Linux VM
   

Figure : Inspecting the WLan Traffic

1. Check the **BSSID, Channel** and **SSID** being used against the approved whitelist to answer the questions regarding these items

*Hint: You can save this information into a file for analysis by clicking on the “Save as…” button in the bottom right.*

Answer the following questions:

#### Question 6: Give the SSID of two APs.

#### Question 7: What is the SSID being used for the device with the BSS Id: Netgear\_45:44:56 (00:1f:33:45:44:56)

#### Question 8: What is the channel being used by the WAP with the BSSID Netgear\_45:44:56?

#### Question 9: How many of these APs in the approved device whitelist?

#### Question 10: Are there any rouge APs (yes/no)? This would be any APs on the network that are NOT on the approved whitelist.

#### Question 11: If rogue wireless access points (WAPs) exist, how many?

1. If you are not continuing to the extension activity, Quit Kali Linux and end your reservation

### Extension ACTIVITY: live capture With Wireshark

**NOTE:** Running Wireshark with root-system privileges and is required for operations that monitor and save (capture) live network traffic. When prompted for the root password, enter **kali** to open and run Wireshark.

Your turn!

1. **Start a Live Network Traffic Capture**

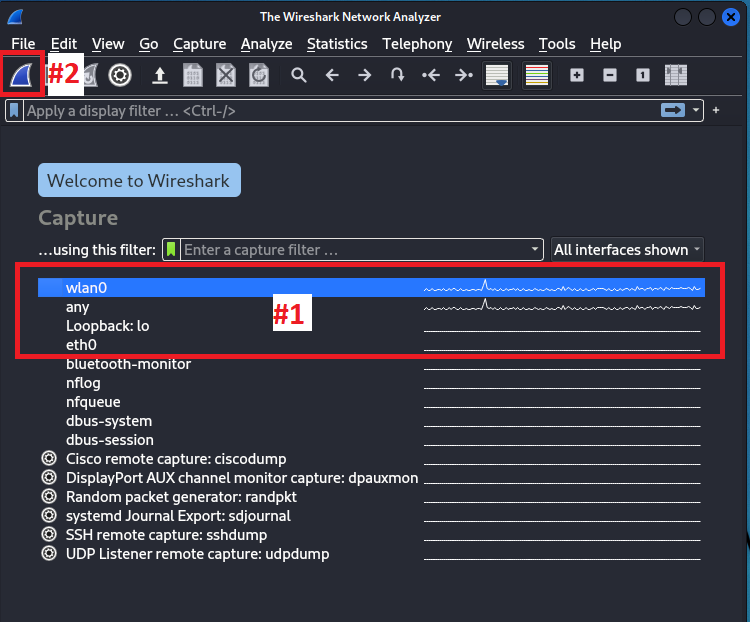
Start traffic capture on the Ethernet (eth0) network interface.

Figure : Starting a live capture in Wireshark. Select interface first (#1) and start capture (#2)

Highlight the “wlan0” or “eth0” interface (Box #1 in Figure 19) depending on which network interface is used to connect to the network on the Raspberry Pi.

Box 3: select “wlan0” or “eth0” in Box 1. Double clicking on the interface will start the capture.

- OR -

Box 3: select “wlan0” or “eth0” in Box 1, and then press the shark fin button highlighted by Box #2

After doing so, the live packet capture will record all packet data traversing the host running Wireshark. Observe for a few moments the traffic that is coming in.

***WARNING:*** *Capturing live packet traffic takes up a very large amount of memory. Never leave a Wireshark capture running. Doing so for just a few minutes, can fill up Gigabytes of system memory or fill up your disk when trying to save. This can make your system unstable or crash Wireshark (often!). Stop Wireshark by hitting the button next to the #1 as shown in* **Error! Reference source not found.***.*

1. To generate network traffic, open a web browser and navigate to a webpage.



Figure : Icon to open up a web browser at top of screen in Kali

1. After capturing some network traffic, stop the capture. To stop the capture, use the red button - OR - under the menu Capture -> Stop

Figure : Generating web traffic and capturing it in Wireshark

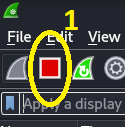
**Stop Capture Button:** This red square button stops the current capture. Once you click this, you can analyze the data and have the option to save it as a .pcap file (a file containing captured packet data) for further analysis or exporting.

Figure : How to stop a live network capture in Wireshark

***NOTE:*** *Once you capture data, you can save it by simply opening* ***File / Save*** *and giving it a file name. By default, it will save the newer file format called .pcapng, but you can also save in the more classic .pcap format.*

Reflection question: How do the DNS queries and responses relate to the web page that you searched for? Was there more than one DNS entry? Hint: you can filter the DNS packets by entering “DNS” into the filter string field. This field shows as green in Figure 21.

# WHAT TO SUBMIT

Submit your answers the questions below.

#### Question 1: What is the *DESTINATION* *port* of the packet in question? Hint the DESTINATION IP address IS 65.165.167.86. The SQL Server Browser service listens on this port for incoming connections.

#### Question 2: Name the protocol used to spread the SQL Slammer Worm in this packet.

#### Question 3: In Packet No. 5, what URL was queried for its DNS information?

#### Hint: look under “Domain Name System (response)” and expand the “Queries” tab.

#### Question 4: In Packet No. 5 (and all of these DNS packets), what protocol is used?

#### Question 5: What is the IP address of the Domain Name Server (i.e. the computer that handles the phonebook lookups)? This computer is the source of the DNS responses (answers).

#### Question 6: Give the SSID of two APs.

#### Question 7: What is the SSID being used for the device with the BSS Id: Netgear\_45:44:56 (00:1f:33:45:44:56)

#### Question 8: What is the channel being used by the WAP with the BSSID Netgear\_45:44:56?

#### Question 9: How many of these APs in the approved device whitelist?

#### Question 10: Are there any rouge APs (yes/no)? This would be any APs on the network that are NOT on the approved whitelist.

#### Question 11: If rogue wireless access points (WAPs) exist, how many?

\*\*Work adapted from the Virginia Cyber Range Wireshark lab and the 2019 UMGC GenCyber Wireless Lab.\*\*