# Intro to Linux

## tcpdump vs Wireshark Lab

# tcpdump vs Wireshark

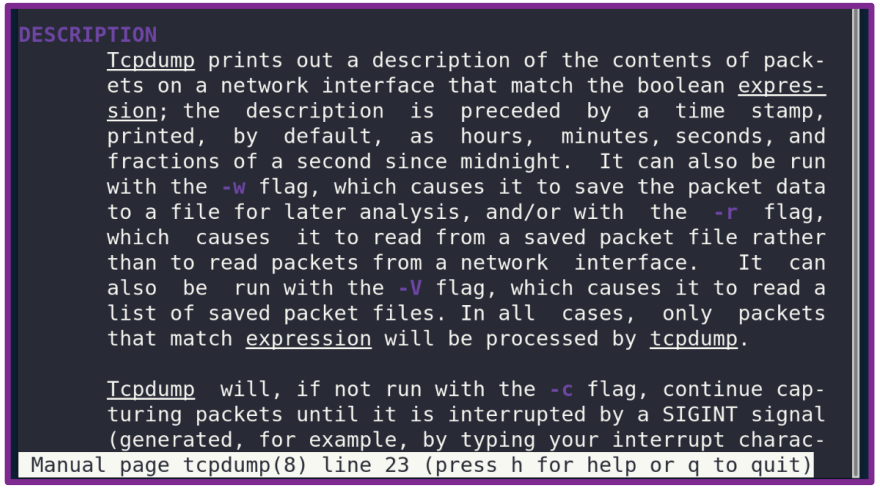
- Materials needed
  - Ubuntu Linux Machine
  - Kali Linux Machine
- Software Tools used
  - tcpdump
  - Wireshark
  - JuiceShop

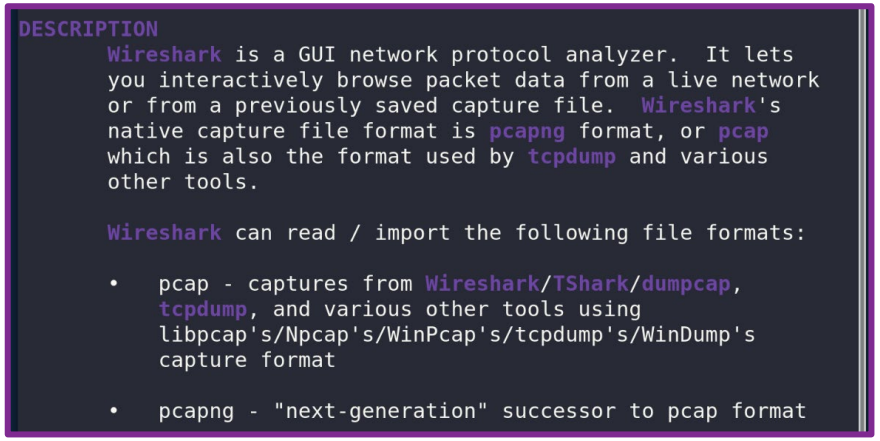
# Objectives Covered

- Linux+ Objectives (XKO-005)
  - Objective 1.5 - Given a scenario, use the appropriate networking tools or configuration files
    - Network Monitoring
      - tcpdump
      - Wireshark

# tcpdump and Wireshark

- Tcpdump is a CLI-based packet analyzer.
  - Monitors incoming and outgoing packets
  - Lists source and destination details
- Wireshark is a GUI-based packet analyzer that offers a user-friendly interface.
  - Captures and analyzes network packets
  - It also offers advanced features, such as packet filtering, protocol decodes, and customizable display options.




CYBER.ORG

# tcpdump vs Wireshark Overview

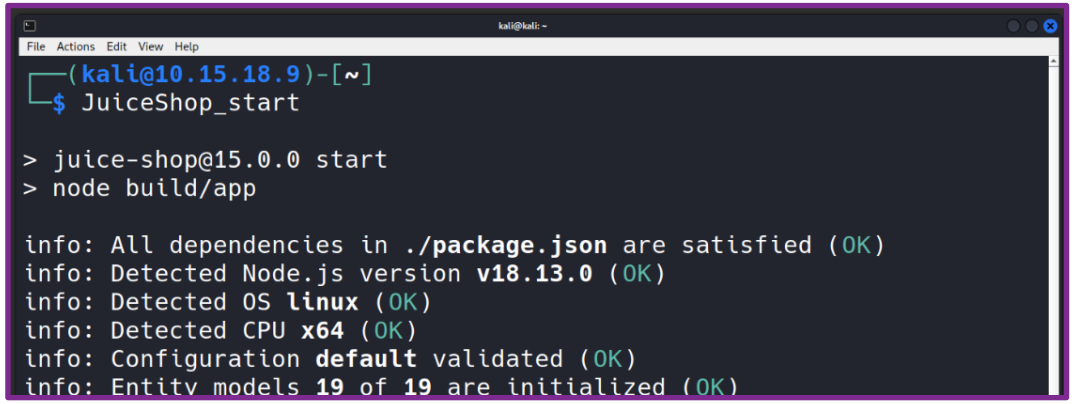
1. Start-up the JuiceShop web app on Kali
2. Capture network packets with tcpdump and Wireshark on Ubuntu
3. Interact with the JuiceShop web app
4. View the packets results from tcpdump and Wireshark

# Setup Environments

- Log into your range
- Once logged in, right click on your browser's tab for the range and click duplicate to have two tabs or windows open
- Open the Ubuntu Linux Environment in one tab
  - You should be on your Ubuntu Linux Desktop
- Open the Kali Linux Environment in the other tab
  - You should be on your Kali Linux Desktop

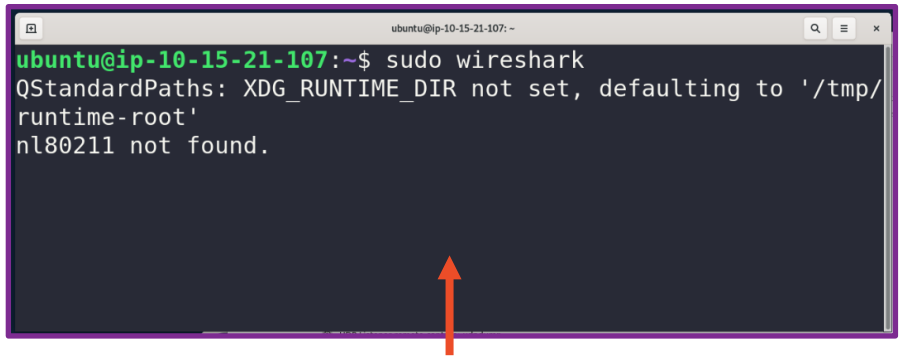
# Start the Juice Shop Application

- Move to your Kali machine
- You will need the Kali IP Address so use the command **`hostname -I`** or take note of it from the terminal or browser tab
- Open a terminal by clicking the white and black icon on the dashboard on the left.
- Use the following to start Juice Shop
- **`JuiceShop_start`**

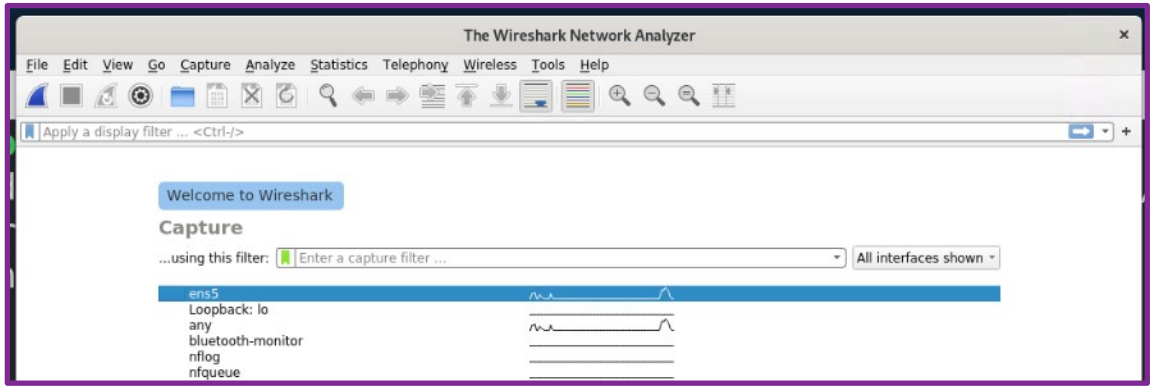


# Move to Ubuntu for Wireshark Setup

- Move to your Ubuntu machine
- Open a terminal by clicking the white and black icon on the dashboard.
- Use the following to open Wireshark
- **`sudo wireshark`**

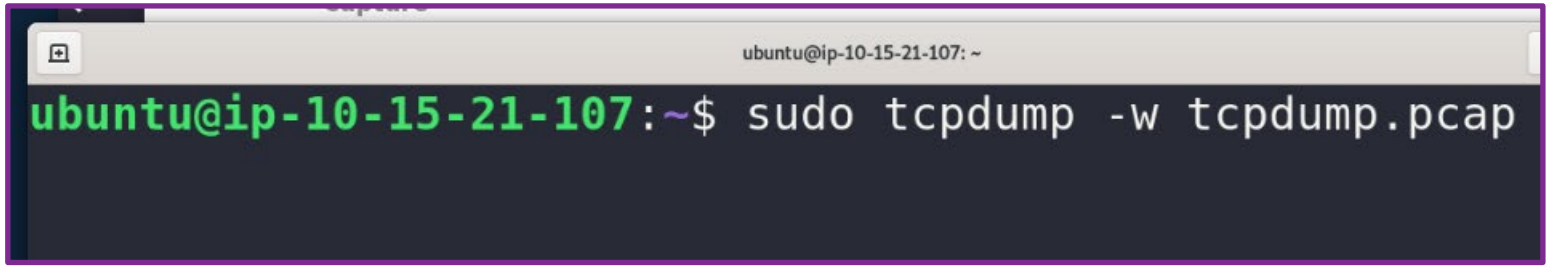



Leave this terminal window open



# tcpdump Setup

- Open a new terminal by right clicking the white and black icon on the dashboard and selecting “New Window.”
- Type the following command but do NOT hit [Enter] right now.
- **`sudo tcpdump -w tcpdump.pcap`**
- This commands starts capturing and writes the data to a file named “tcpdump.pcap.”




Do not hit [Enter] just yet!

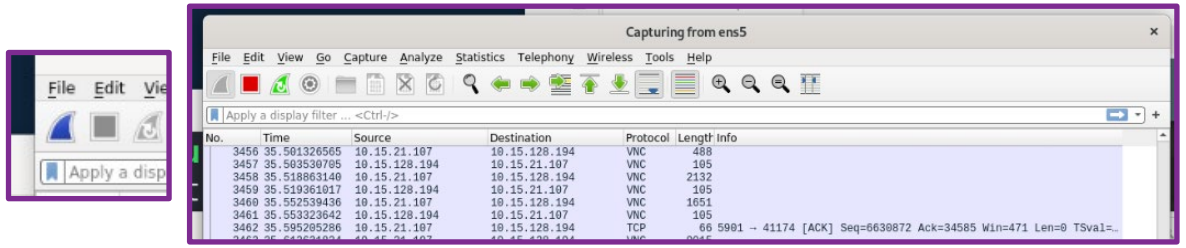
# Open the Browser and Start Capturing

- Open Firefox by clicking the icon on the dashboard.
- While Firefox is opening, begin capturing packets:
  - Return to the Wireshark window and click the blue fin to start packet capturing there.
  - Return to terminal with the tcpdump command and hit [Enter] to start packet capturing there.
- Once the browser loads, navigate to `<Kali_IP_Address>:3000`
- After the page loads, click login under account on the top right side and login using the credentials admin@juice-sh.op and admin123 as the password.

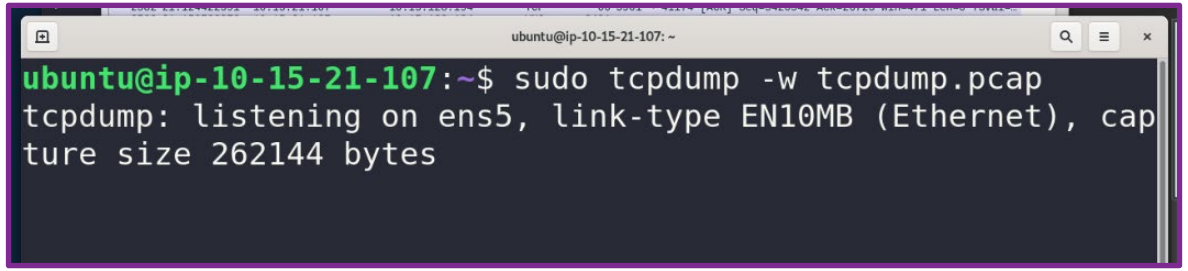
*Note this will be a fast-paced process. It is diagramed on the following slide to assist.

# Diagram of the Process

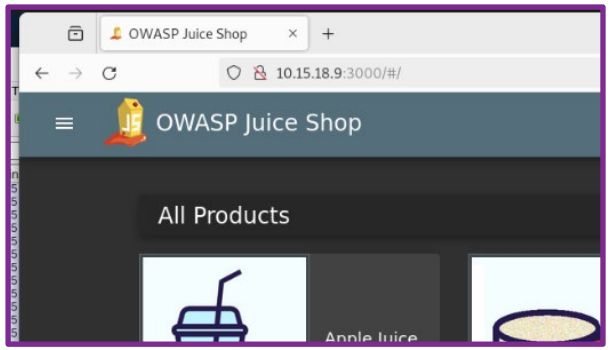
Step 1: Click the blue fin to start capturing in Wireshark



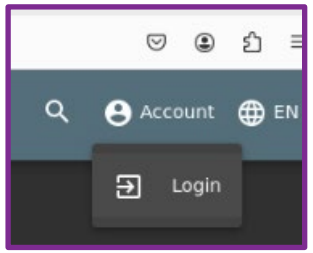

Step 2: Hit [Enter] to start capturing with tcpdump

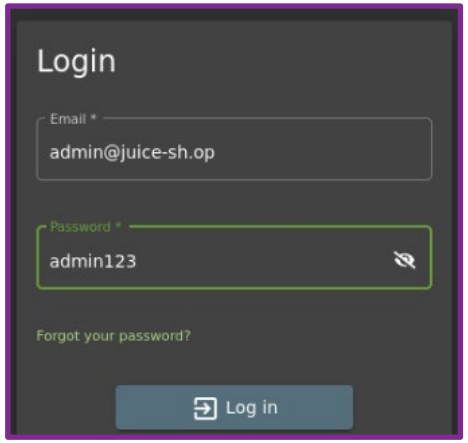



Step 3: Navigate to <Kali_IP_Address>:3000




Step 4: Login to JuiceShop under Account using the credentials:
admin@juice-sh.op
admin123



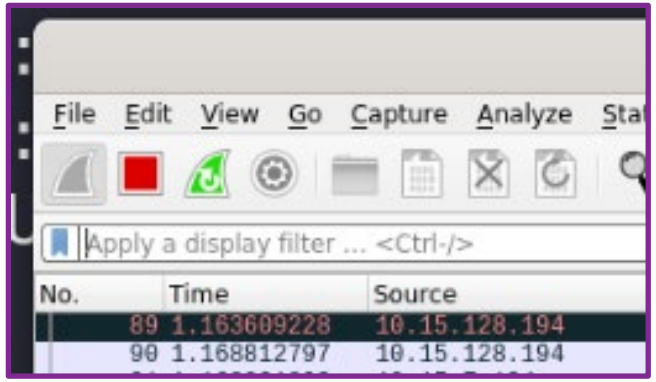




CYBER.ORG

# Stop Capturing

- In the terminal running tcpdump, use CTRL+C to stop the process and save the file.
- In the Wireshark window, click the red square to stop capturing the files.

```
ubuntu@ip-10-15-21-107:~$ sudo tcpdump -w tcpdump.pcap
tcpdump: listening on ens5, link-type EN10MB (Ethernet), cap
ture size 262144 bytes
^C3826 packets captured
3831 packets received by filter
0 packets dropped by kernel
ubuntu@ip-10-15-21-107:~$
```

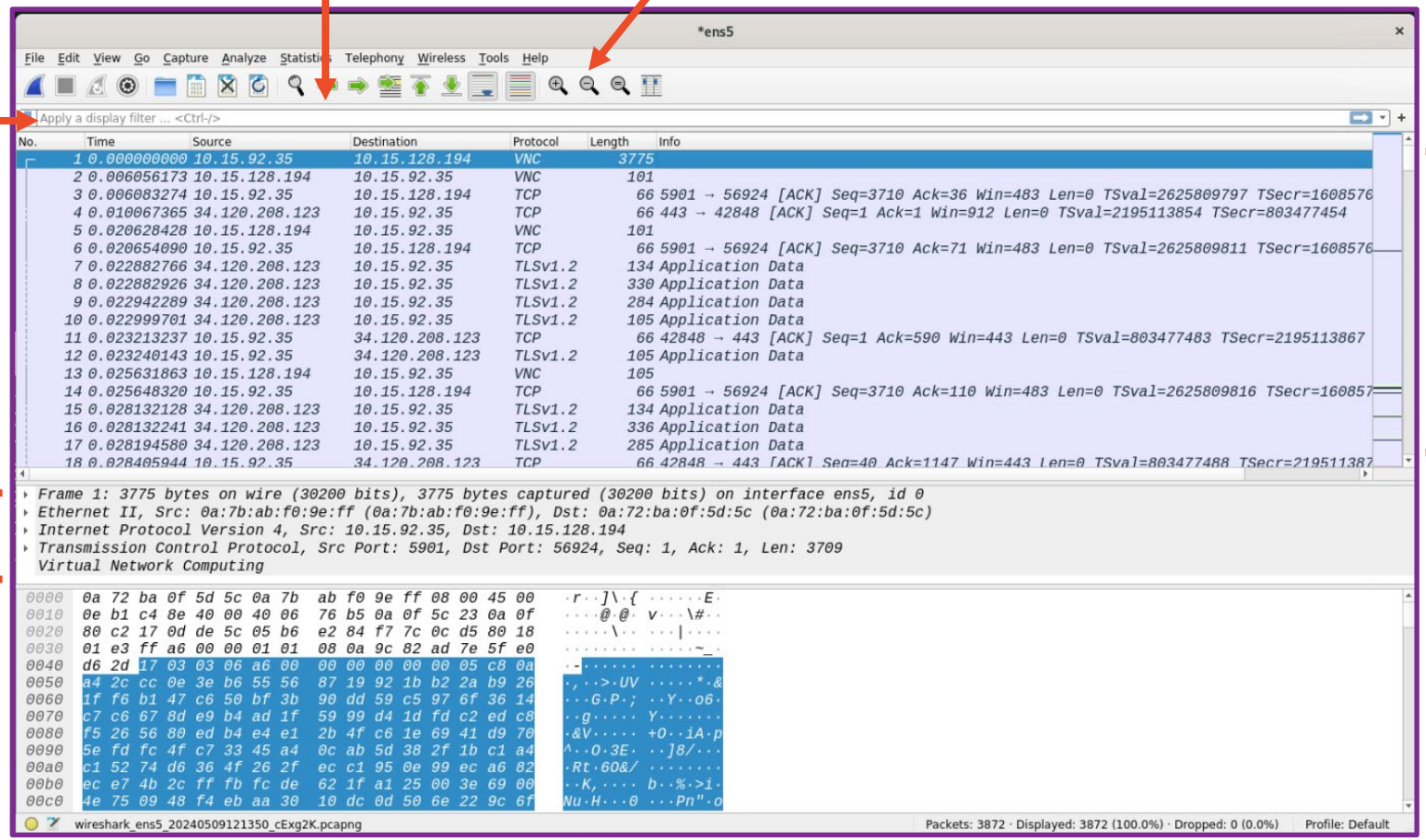


# Packets, Bytes, & Protocols… Oh my!

Search option which allows searching packets, details, strings, and more

Zoom options

Filter bar which can filter by IP address, protocol, and more



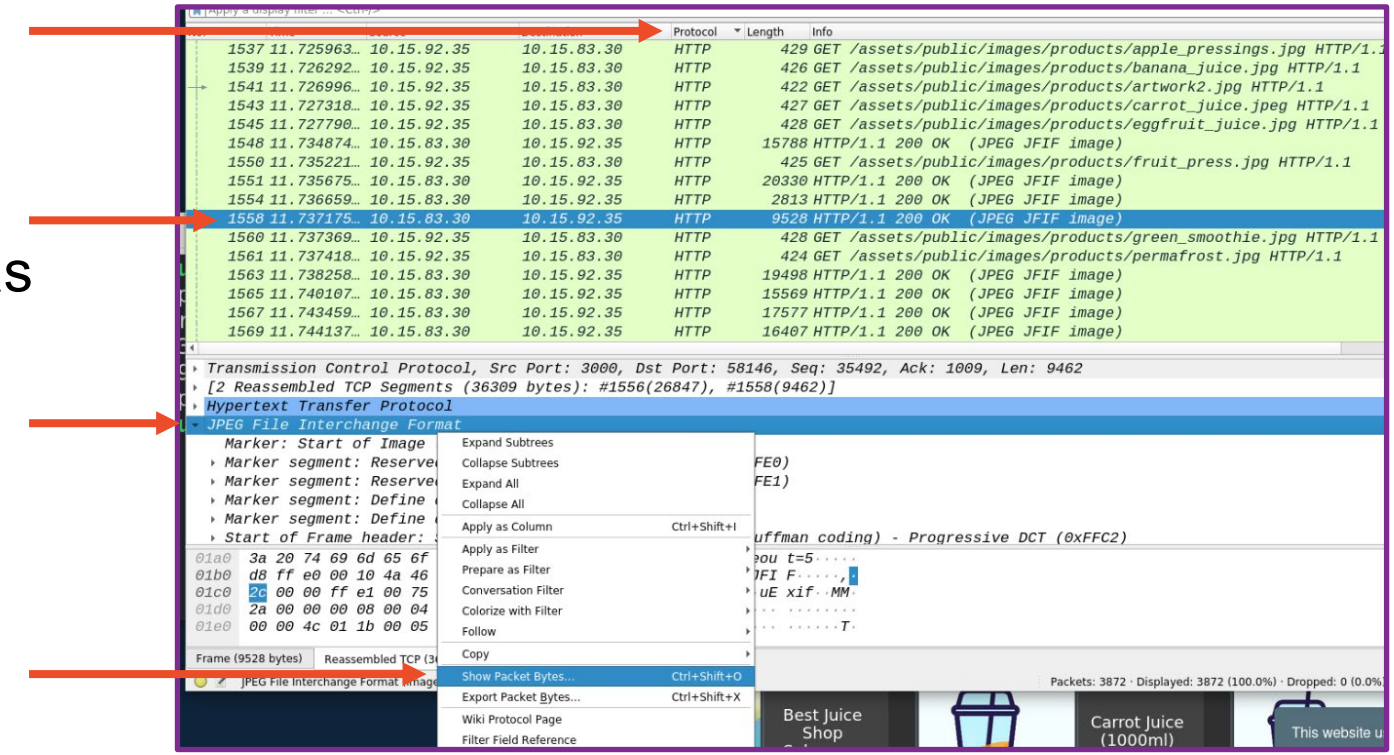

The “Packet List” pane use to view packets which can be sorted by clicking the column headers

Packet Details

Packet Bytes

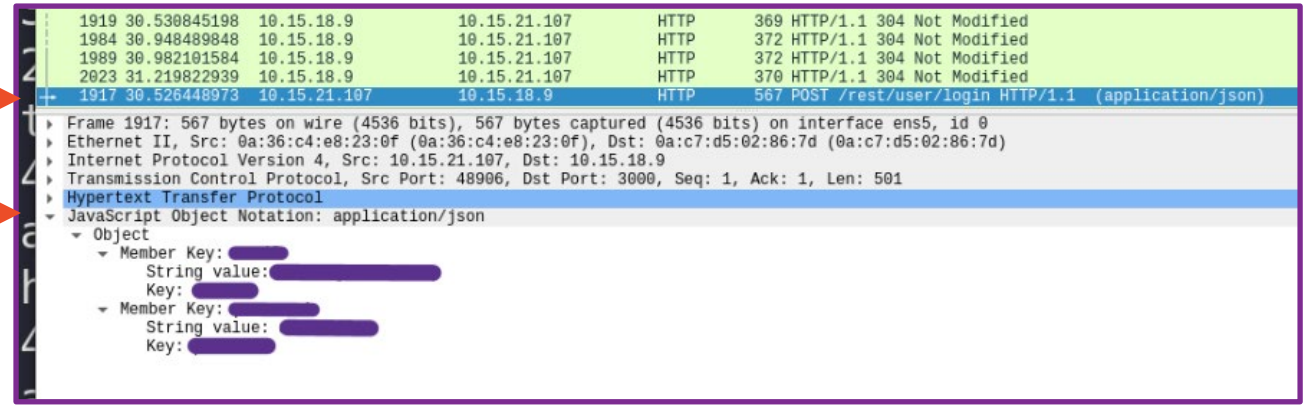
# Analyzing the Wireshark Capture

- Start off by clicking the protocol column to sort the packets alphabetically by protocol
- Scroll down until you see the http packets and try to find one that has “(JPEG JFIF image)” in the info section of the packet
- In the details of the packet, scroll down to JPEG File Interchange Format, right click and select “Show Packet Bytes…”
- What appears?



# Locating the Login from Wireshark

- While the packets are still sorted by protocol, locate the http packet that is a POST and “/rest/user/login” in the info section of the packet
- In the details of the packet, scroll down to JavaScript Object Notation and expand the sections
- What appears?

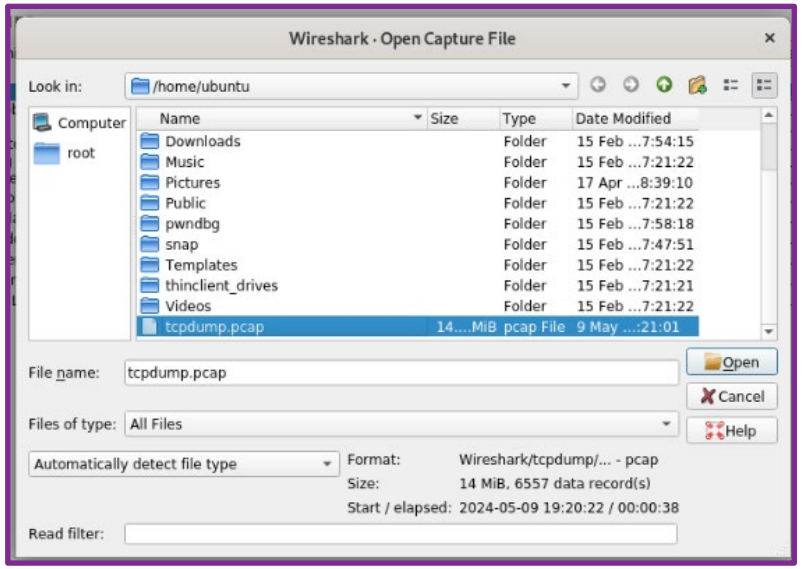



*Note this appears because JuiceShop is meant to mimic a poorly secured web app. Hopefully, web apps use encryption and techniques to hide this information.

# Analyzing the tcpdump Packets

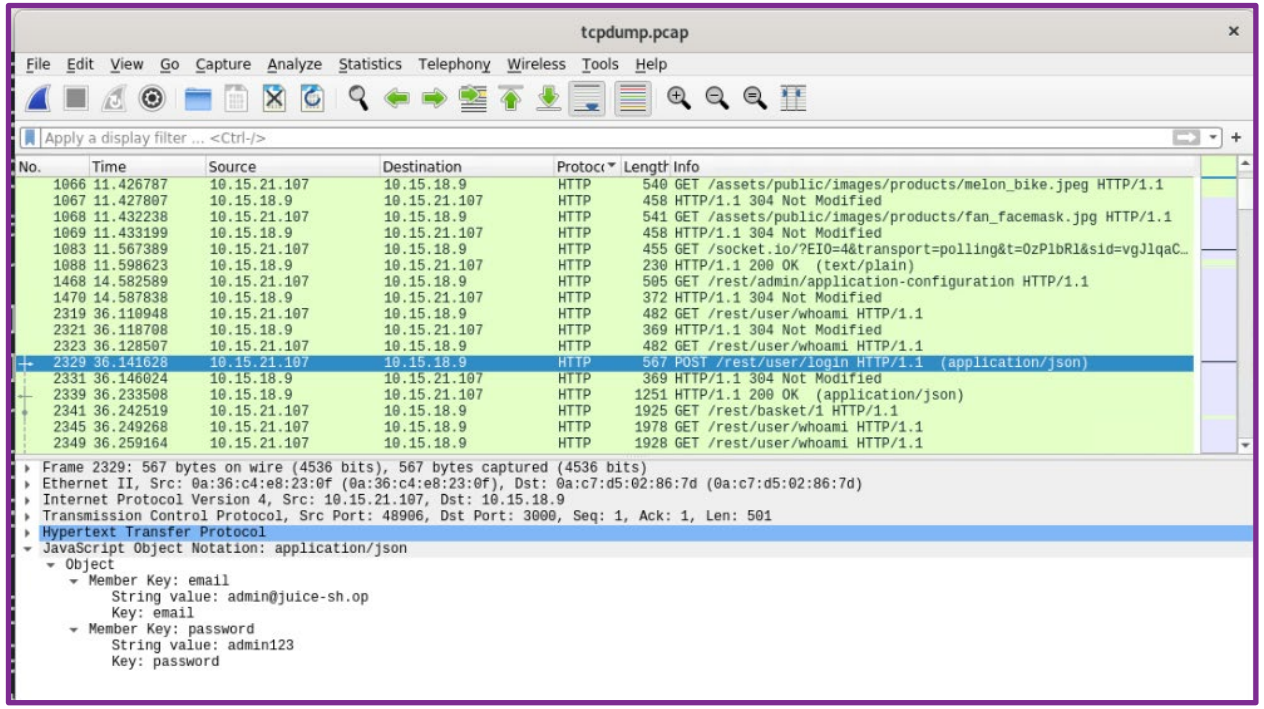
- tcpdump packets can be viewed directly in the terminal using the command **`tcpdump -r tcpdump.pcap`**
- However, this is not user friendly, nor does it give you the details that Wireshark allows.
- In Wireshark, click File → Open → tcpdump.pcap

```
19:20:53.817859 IP 23.185.0.2.https > 10.15.50.118.43428: Flags [P.], seq 105683
1:1063076, ack 5904, win 312, options [nop,nop,TS val 179276001 ecr 1790035227],
 length 6245
19:20:53.817869 IP 10.15.50.118.43428 > 23.185.0.2.https: Flags [.], ack 1063076
, win 11076, options [nop,nop,TS val 1790035229 ecr 179276001], length 0
19:20:53.880808 IP 10.15.50.118.5901 > 10.15.128.194.38574: Flags [.], seq 19398
38:1948787, ack 60102, win 484, options [nop,nop,TS val 1908689766 ecr 200395180
1], length 8949
19:20:53.902238 IP 10.15.50.118.5901 > 10.15.128.194.38574: Flags [.], seq 19487
87:1957736, ack 60102, win 484, options [nop,nop,TS val 1908689788 ecr 200395180
1], length 8949
19:20:53.902425 IP 10.15.128.194.38574 > 10.15.50.118.5901: Flags [.], ack 19577
36, win 443, options [nop,nop,TS val 2003952032 ecr 1908689766], length 0
19:20:53.907775 IP 10.15.50.118.5901 > 10.15.128.194.38574: Flags [.], seq 19577
36:1966685, ack 60102, win 484, options [nop,nop,TS val 1908689794 ecr 200395203
```



# Analyzing the tcpdump file with Wireshark

- Once the file is opened, notice it looks like the capture from Wireshark.
- You can find the same packets that exchanged data and information including images and the login credentials
- The main difference is tcpdump allows a quick way to start capturing packets through terminal



# Wrap-up

- Wireshark and tcpdump both allow packets to be captured and analyzes from a network
- Wireshark is GUI-based and has several built-in tools to assist in capturing and analyzing data
  - Clicking help and exploring the Manual pages gives you several additional options
- tcpdump is CLI-based and allows a quick method to capture packets in terminal
  - Use **`man tcpdump`** to look at additional options such as specifying connections, ports, or duration.