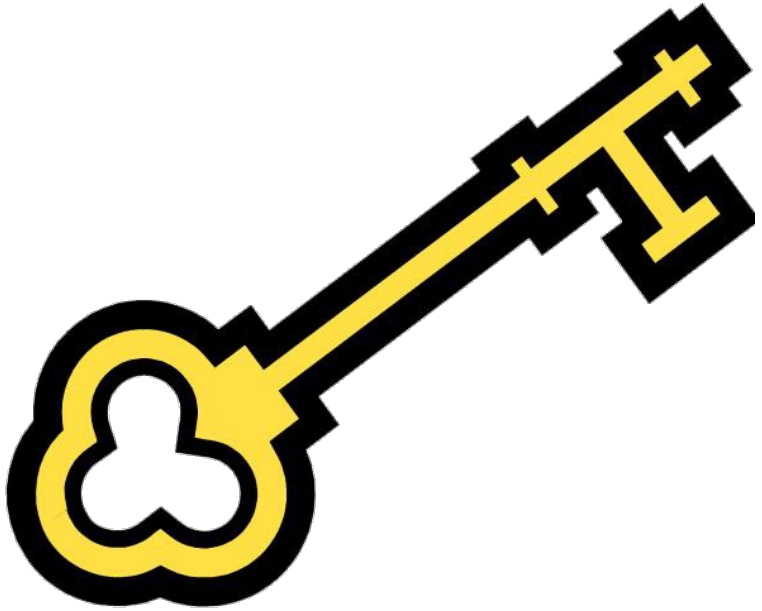
AskCyPert

Packet Sniffing Lab



CAC Center for Cloud and Autonomic Computing

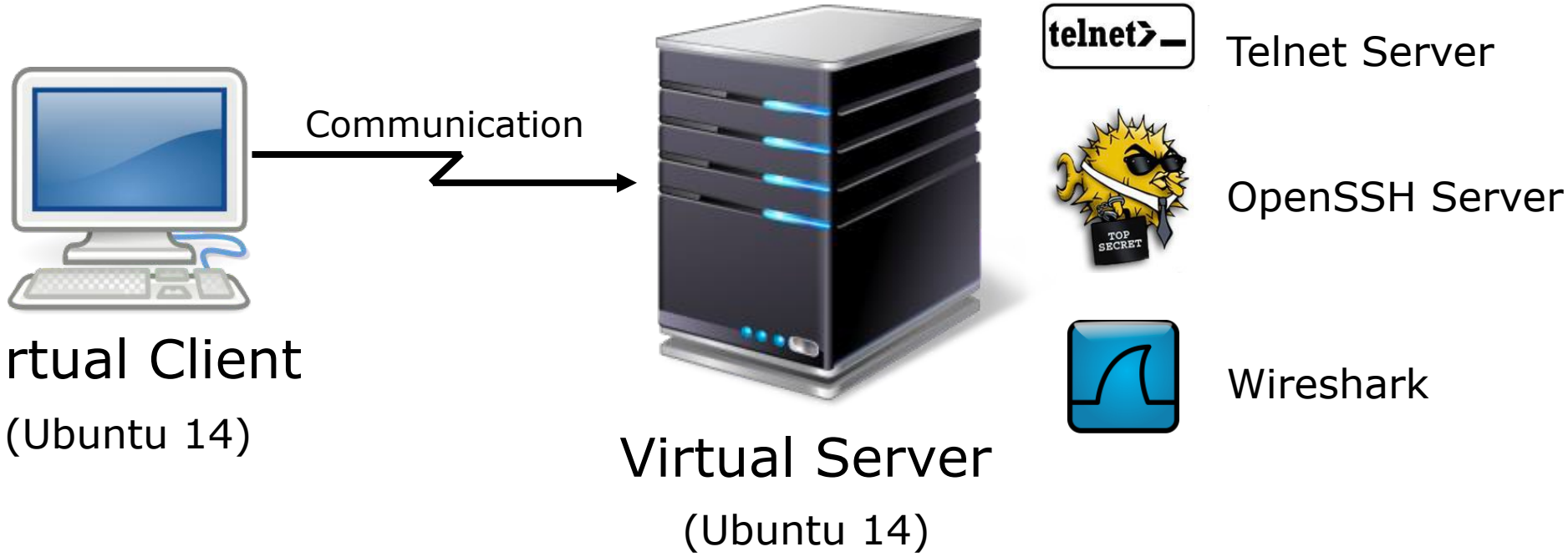
NATIONAL SCIENCE FOUNDATION

Purpose

- Understanding network packets and protocols
- Using Wireshark to capture and analyze network packets

Virtual Lab Setup

- Two VM instances within the same subnet will be used



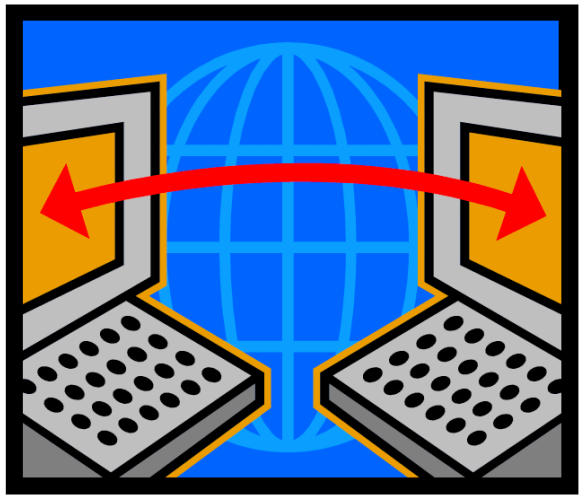
Lab Structure

- The *Packet Sniffing* lab consists of 5 experiments
  1. Telnet
  2. SSH
  3. TCP Traffic Analysis
  4. UDP Traffic Analysis

Lab Software Tools

For this lab we will be using the following tools:

- **Telnet Client/Server:** The client establishes a remote connection to the server using Telnet protocol.
- **SSH Client and Server:** The SSH client establishes a remote connection to the SSH server using the *Secure Shell (SSH)* protocol.



Lab Software Tools

- **Wireshark:** Analyzes all packets of a network interface
  - We will use Wireshark to analyze all communications between the client and the server VMs
  - Wireshark will obtain all transferred information, including client's username and password
  - Confidentiality property of cybersecurity will be violated

AskCyPert

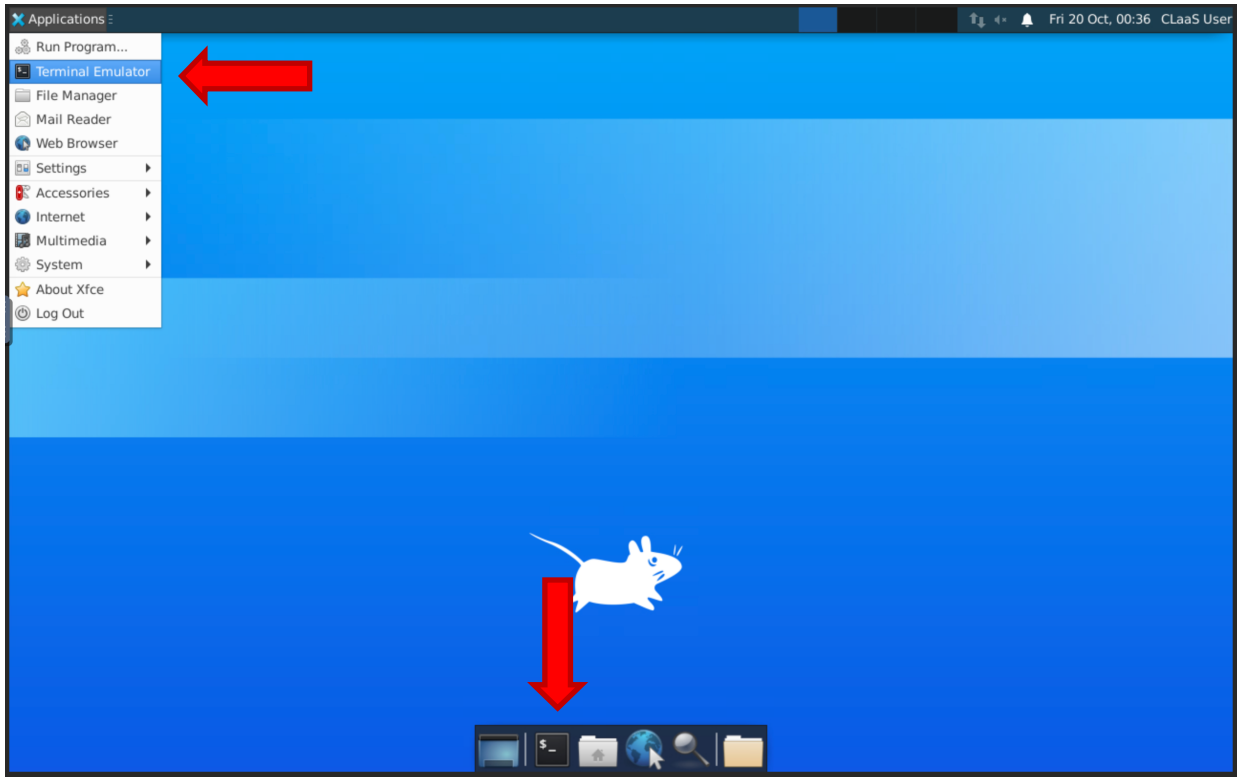
CAC Center for Cloud and Autonomic Computing

Experiment 0:
Getting ready to start

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Open a terminal
  - For this lab we will be using the terminal.
  - There are two ways to open it.
    - From the menu
    - Or by clicking the icon on the dock:

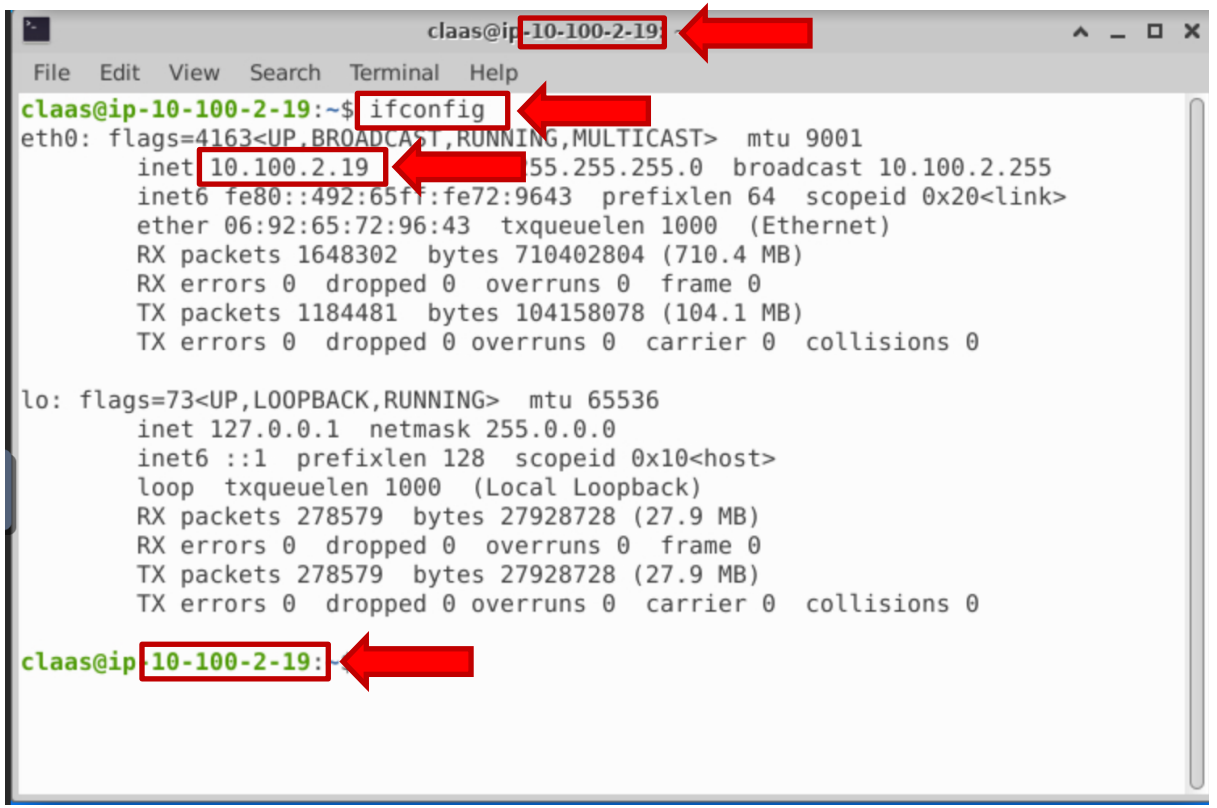


Experiment Instructions

- Step 2: Get the IP addresses
  - We can see the IP address as soon as we open the terminal
  - Or by typing

    ```
    ifconfig
    ```

  - *You will need the IP of the two VMs, for the rest of the lab.*



AskCyPert

CAC Center for Cloud and Autonomic Computing

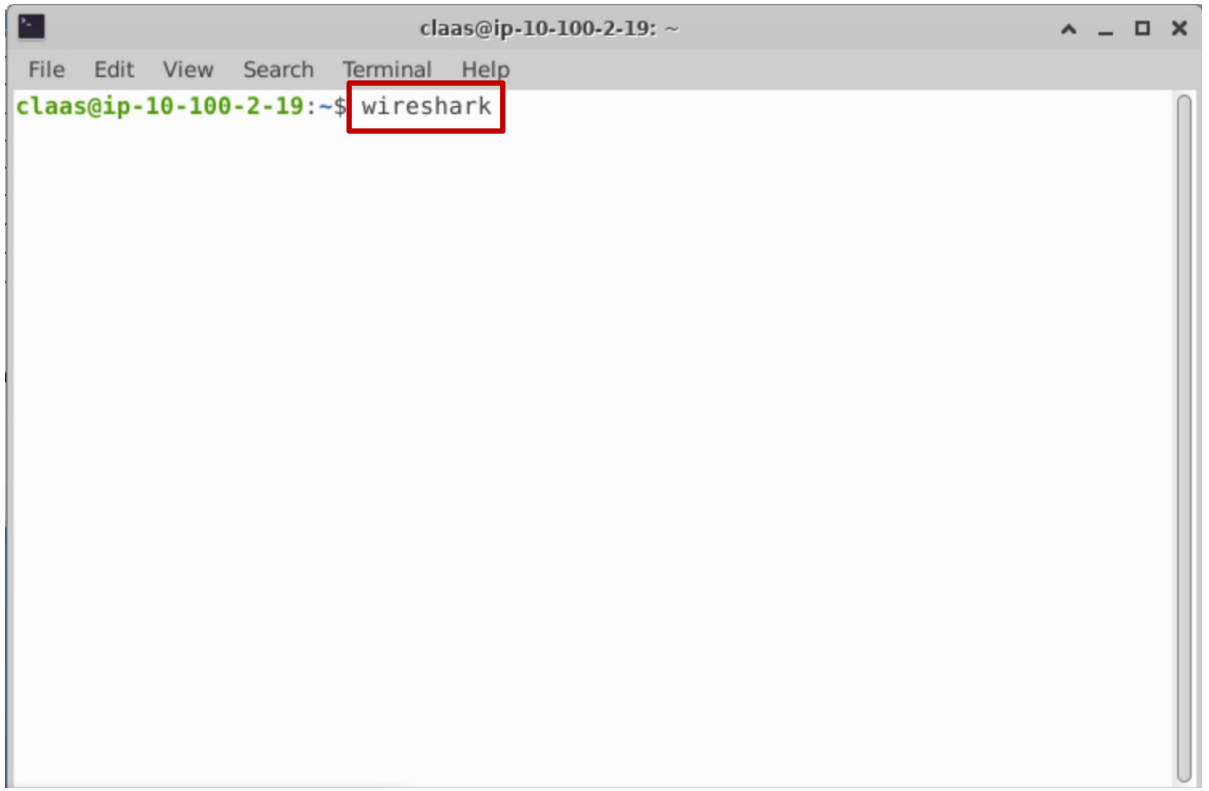
Experiment 1: Telnet

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

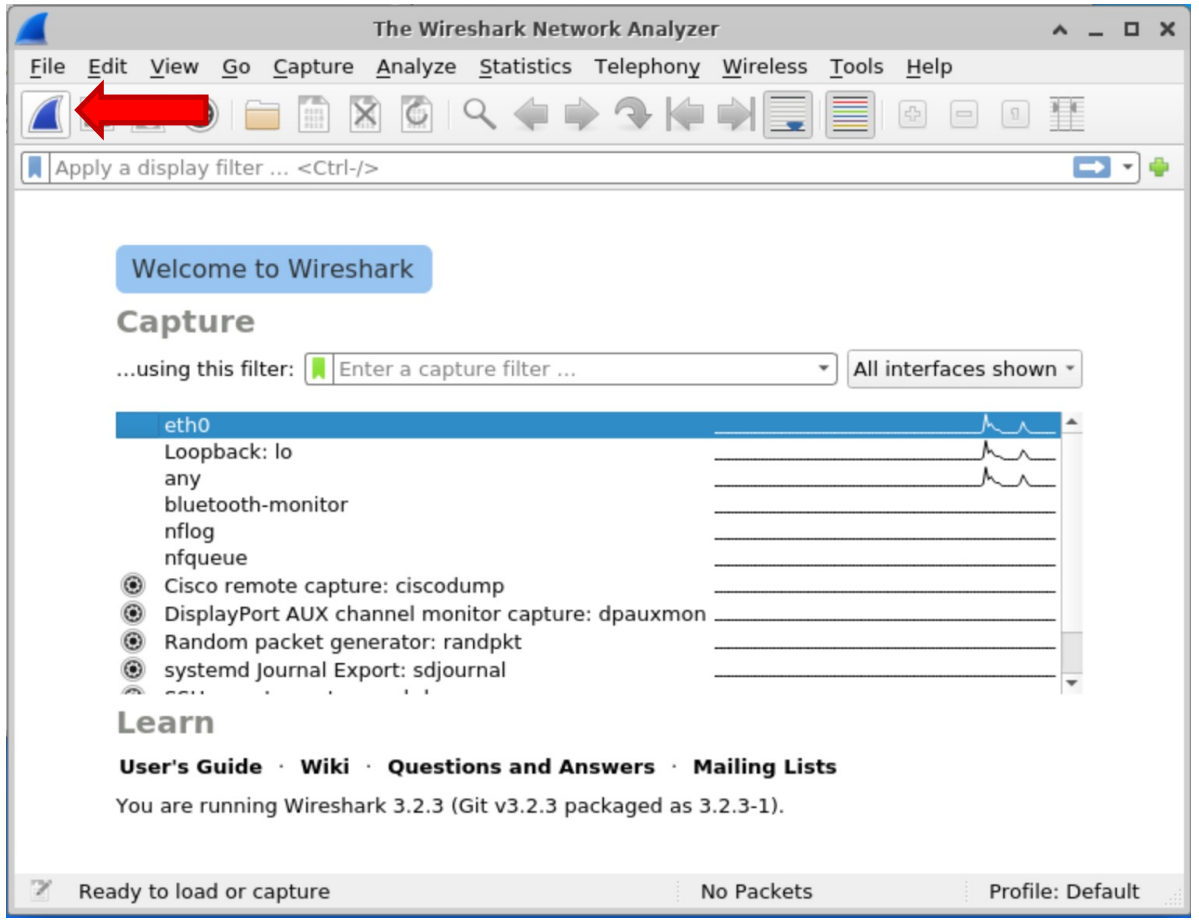
- Step 1: Open Wireshark
  - On the Server VM
  - Open a terminal and type

```
wireshark
```



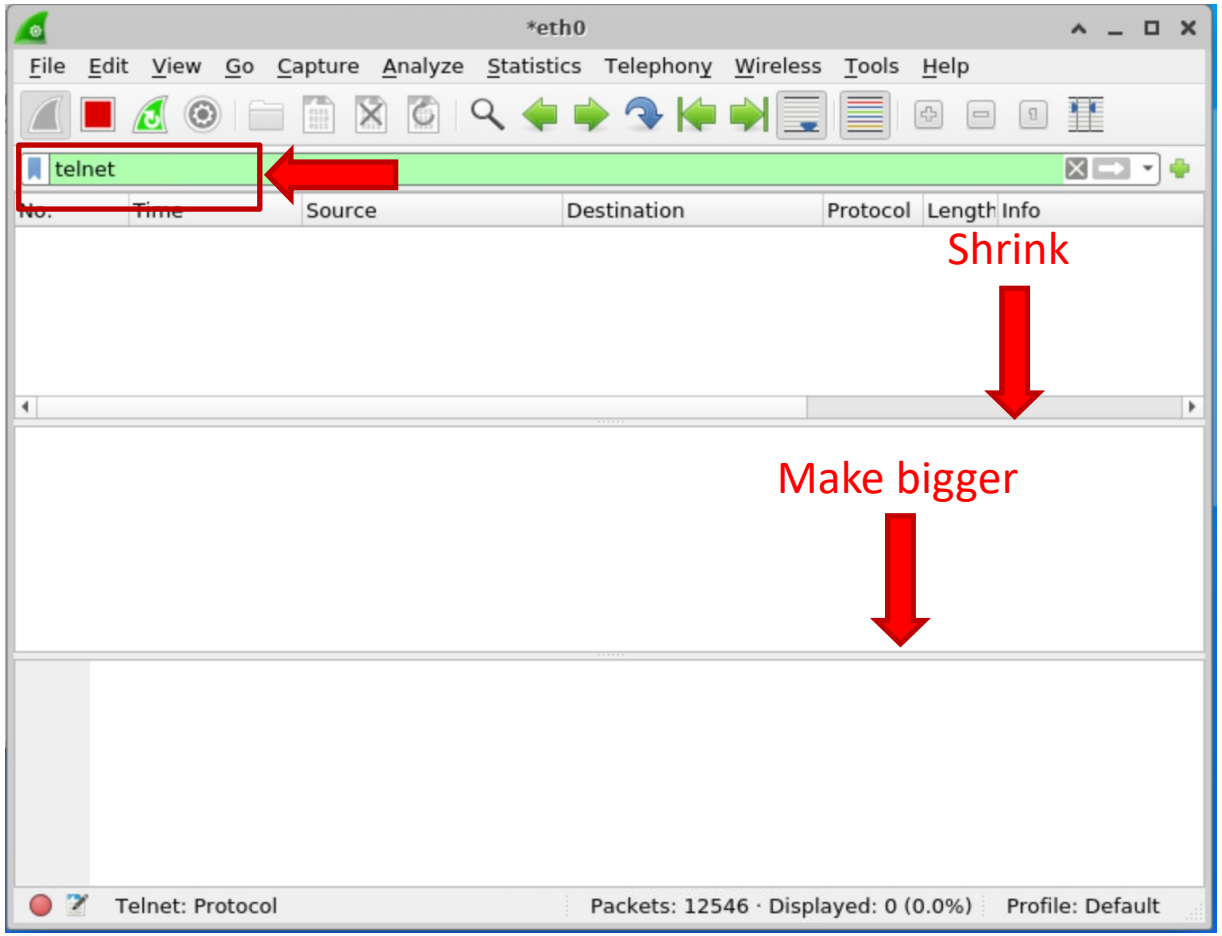
Experiment Instructions

- Step 2: Prepare Wireshark
  - Once Wireshark is open select the *eth0* interface
  - Click the blue button to *Start capturing packets*



Experiment Instructions

- Step 3: Filter Telnet packets
  - In the filter field, type *telnet* to filter only telnet packets
  - Adjust the windows, this way we'll be able to see the packets better

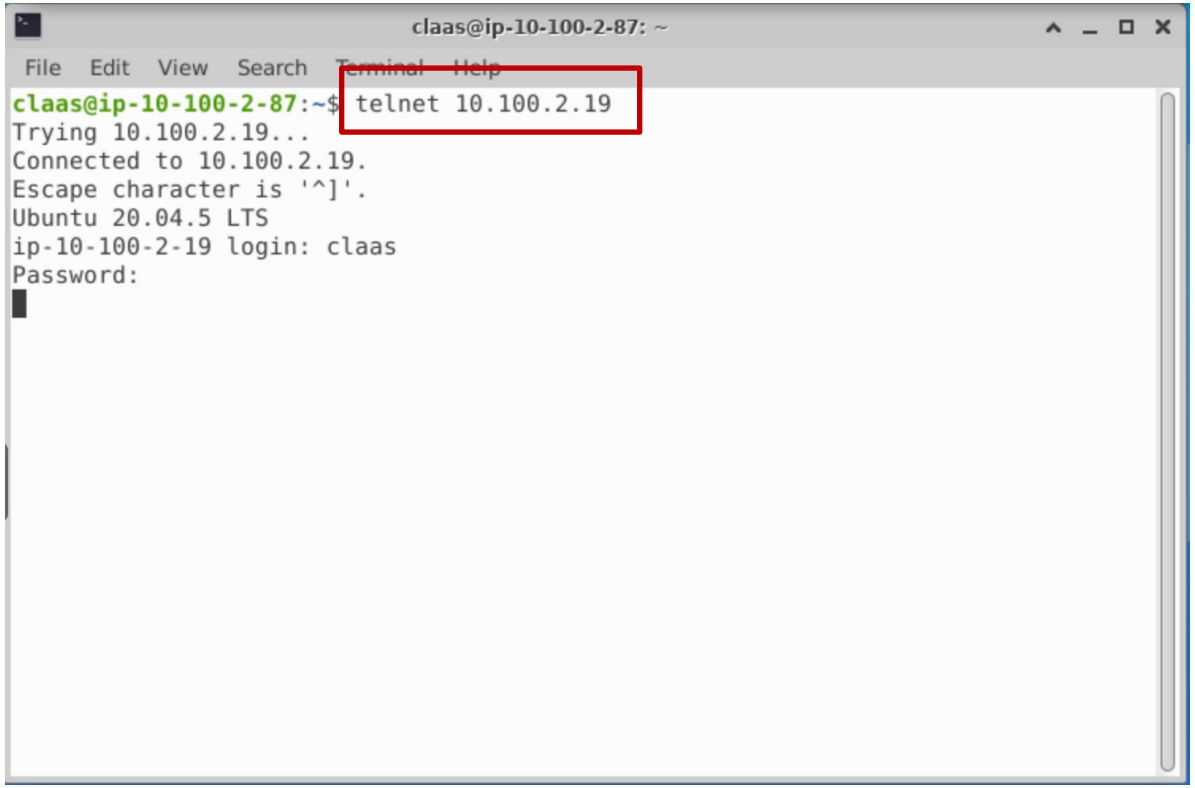


Experiment Instructions

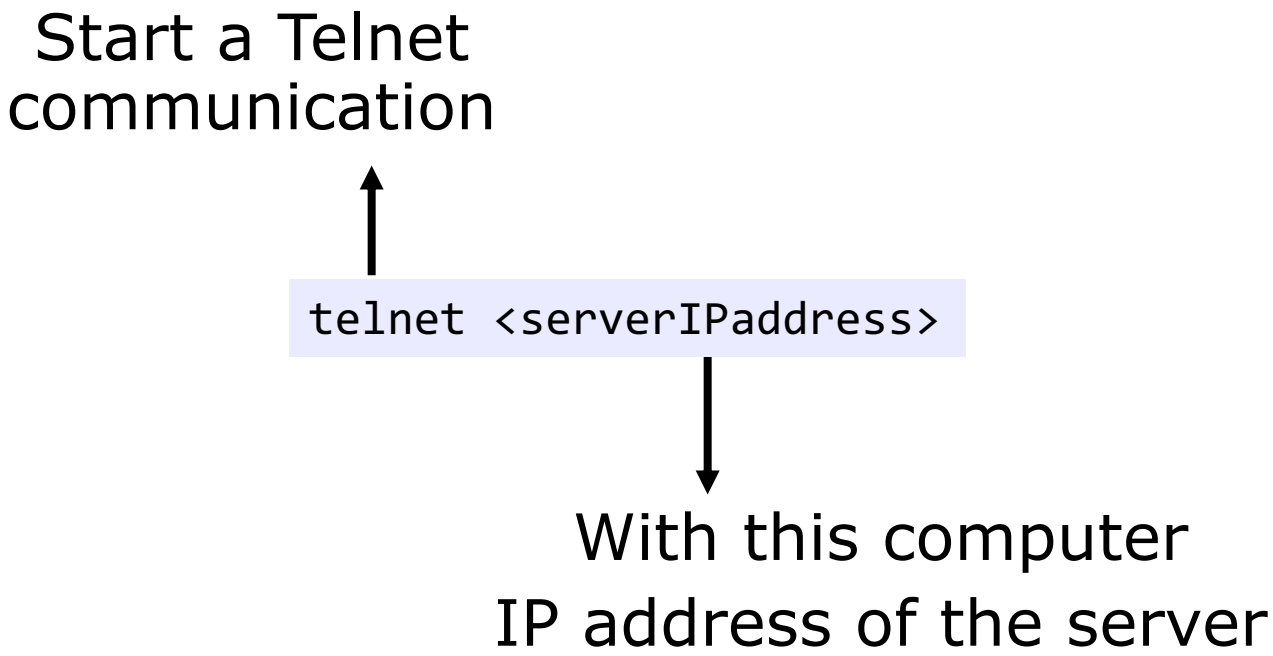
- Step 4: Generate Telnet packets
  - Go back to the Client VM
  - Open a terminal, and type

```
telnet <serverIPaddress>
```

  - Once connected type:
    - Username: *claas*
    - Password: *Claas2022*



Command Explained



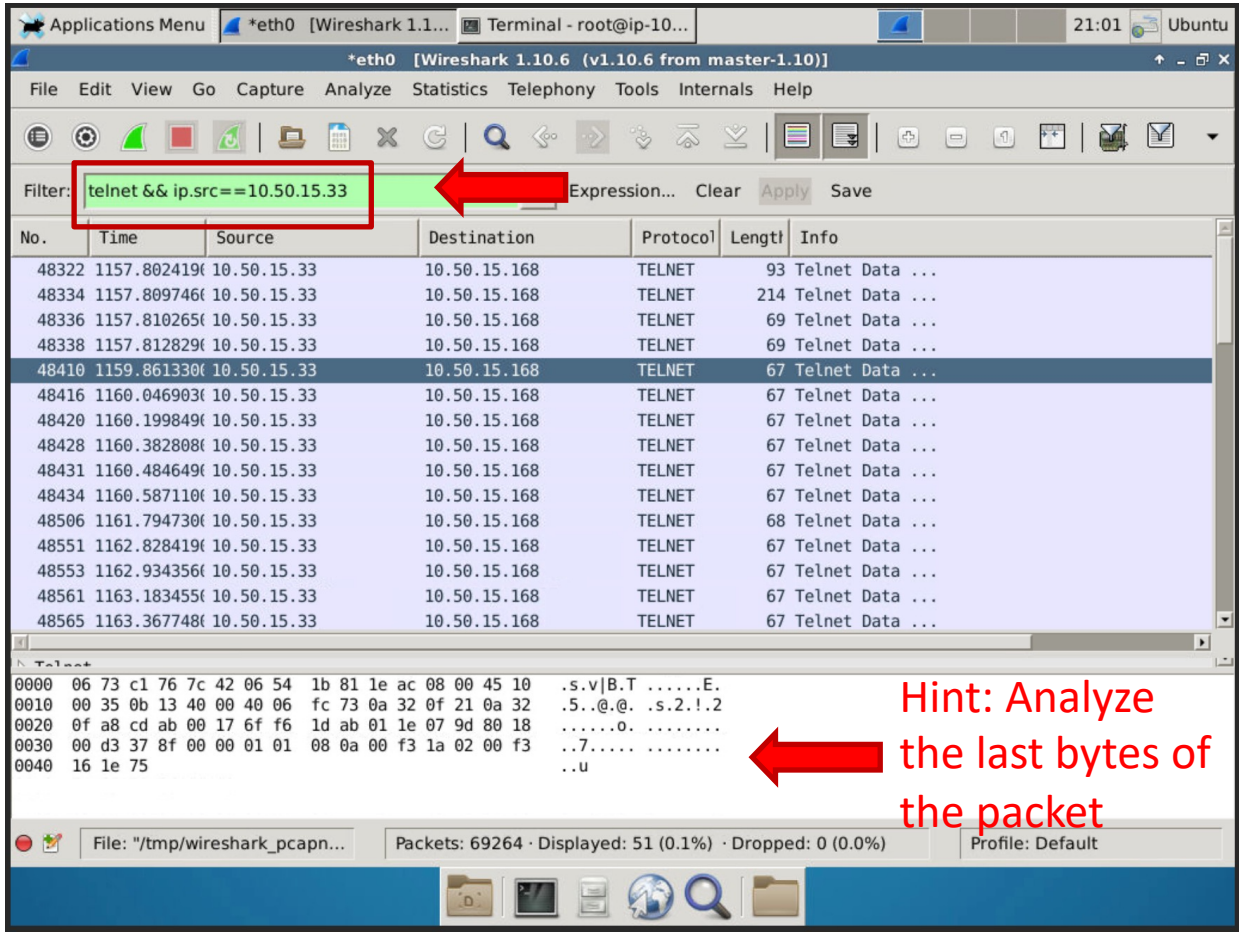
- Exit your Telnet session by pressing **Ctrl+C**
- Or type **exit**

Experiment Instructions

AskCyPert

- Step 5: Analyze Telnet packets
  - Go back to Wireshark in the Server VM
  - Analyze the packets captured from the Telnet session
  - Hint: You might want to filter also by IP, to do this type on the filter field:

```
telnet && ip.src==<clientIPaddress>
```



Experiment Summary

- **Please note**
  - Telnet sends all packets (including username and password) in plaintext
  - An attacker would have no difficulty reading it using Wireshark
  - After retrieving the credentials, the attacker can connect to the server and have the same access privileges as the client

Lab Report

- Analyze the Telnet packets captured by Wireshark and describe them
- Describe the steps and their results in the report
- Obtain the username and password and some commands sent from the client, include them in your lab write-up, and explain how you have obtained them from Wireshark

How do you prevent such attacks?

- This security issue can be remedied if a communication protocol with encryption is used to transfer information between client and server machines.
- Unlike Telnet, the SSH protocol does not transmit data in plaintext. It encrypts transmitted data so that, even if attackers intercept the data, it is incomprehensible and thus still secure.

AskCyPert

CAC Center for Cloud and Autonomic Computing

Experiment 2: SSH

NATIONAL SCIENCE FOUNDATION

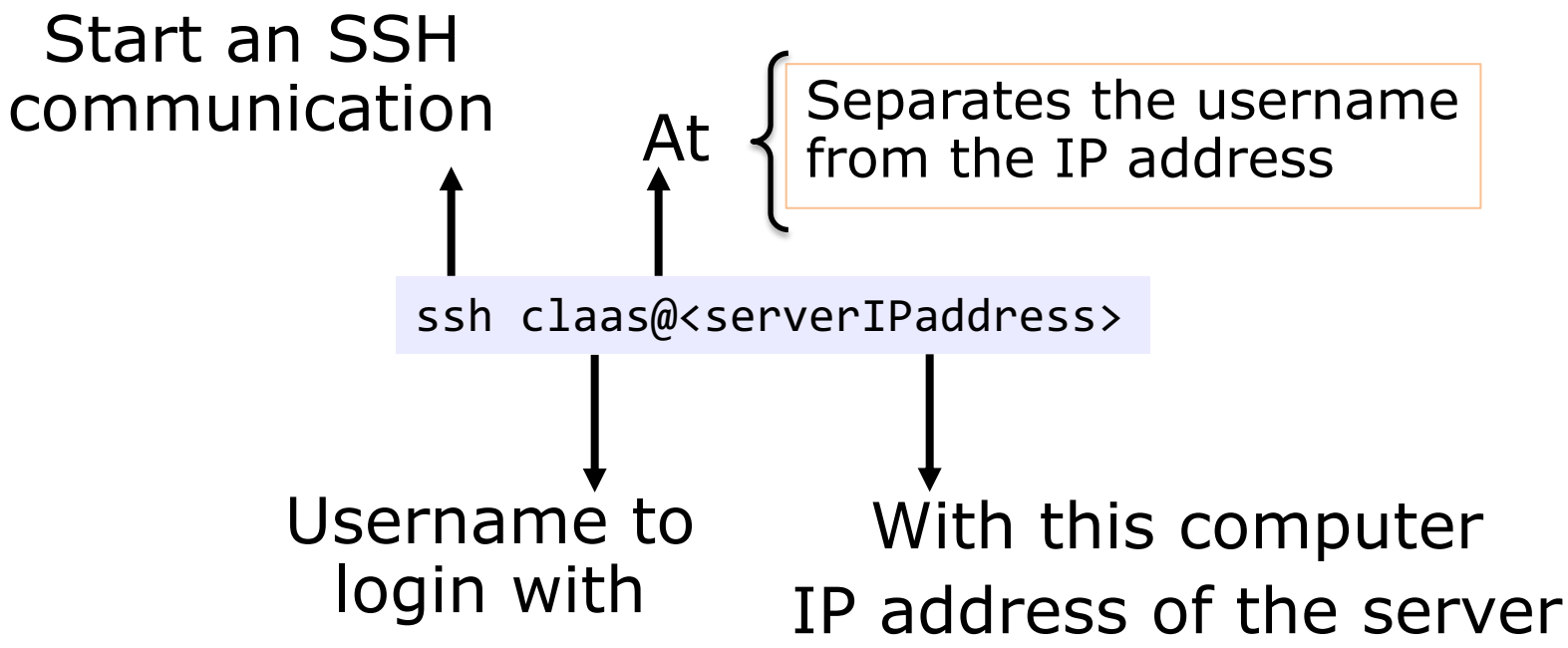
Experiment Instructions

- For this experiment, you will follow the same steps as in the Telnet experiment, with these differences:
  - In step 3 we will filter SSH instead of Telnet packets
  - For step 4, on the terminal you'll type:

```
ssh claas@<serverIPaddress>
```

  - After this, it will ask you if you want to establish a connection, type *yes*, and type the password *Claas2022*
  - Proceed with the next steps

Command Explained



- Exit your SSH session by pressing **Ctrl+C**
- Or type **exit**

Experiment Summary

- **Please note**
  - SSH uses encrypted packets
  - An attacker will fail to understand the contents without decrypting it

Lab Report

- Analyze the SSH packets captured by Wireshark and describe them
- Describe the steps and their results in the report
- Can you obtain a username and password, or any useful information sent via SSH? Justify your answer

Other features of Wireshark

- With Wireshark, you can also analyze the packet structure

- For the next experiments, you won't only view the contents of the packet, but also the multiple layers of encapsulation that go into creating a packet

AskCyPert

Experiment 3: TCP Traffic Analysis

CAC Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Connect to a webpage
  - On the Server VM, you will use Elinks (a web-based browser)
  - Connect to a webpage typing

```
elinks www.google.com
```

  - Exit the terminal-based website by typing **Ctrl+C**

Experiment Instructions

- Step 2: Observe the TCP packets on Wireshark.
  - Go back to Wireshark and type on the filter field:

```
tcp
```

  - Go through the packets in the list and observe the following:
    - Source and destination IPs
    - Source and destination port numbers on both the client and server
    - The packet parameters
    - Maximum and minimum values of these parameters

Experiment Instructions

- Step 3: Change the display filter to *HTTP*
  - Go through the packets in the list and add the following information to your lab report:
    - Describe the HTTP commands and their parameters
    - What are the maximum and minimum values of these parameters?
    - What are the listed HTTP headers and what are their values? (Some HTTP packets may not have headers)

Experiment Summary

- **Please note**
  - The TCP protocol includes error checking and packet ordering information
  - HTTP is a TCP protocol

Lab Report

- List source and destination IPs and port numbers from the captured TCP packets
- List TCP packet parameters and maximum/minimum values

- Describe HTTP commands and their parameters (include max/min values)
- List HTTP headers and their values

AskCyPert

Experiment 4: UDP Traffic Analysis

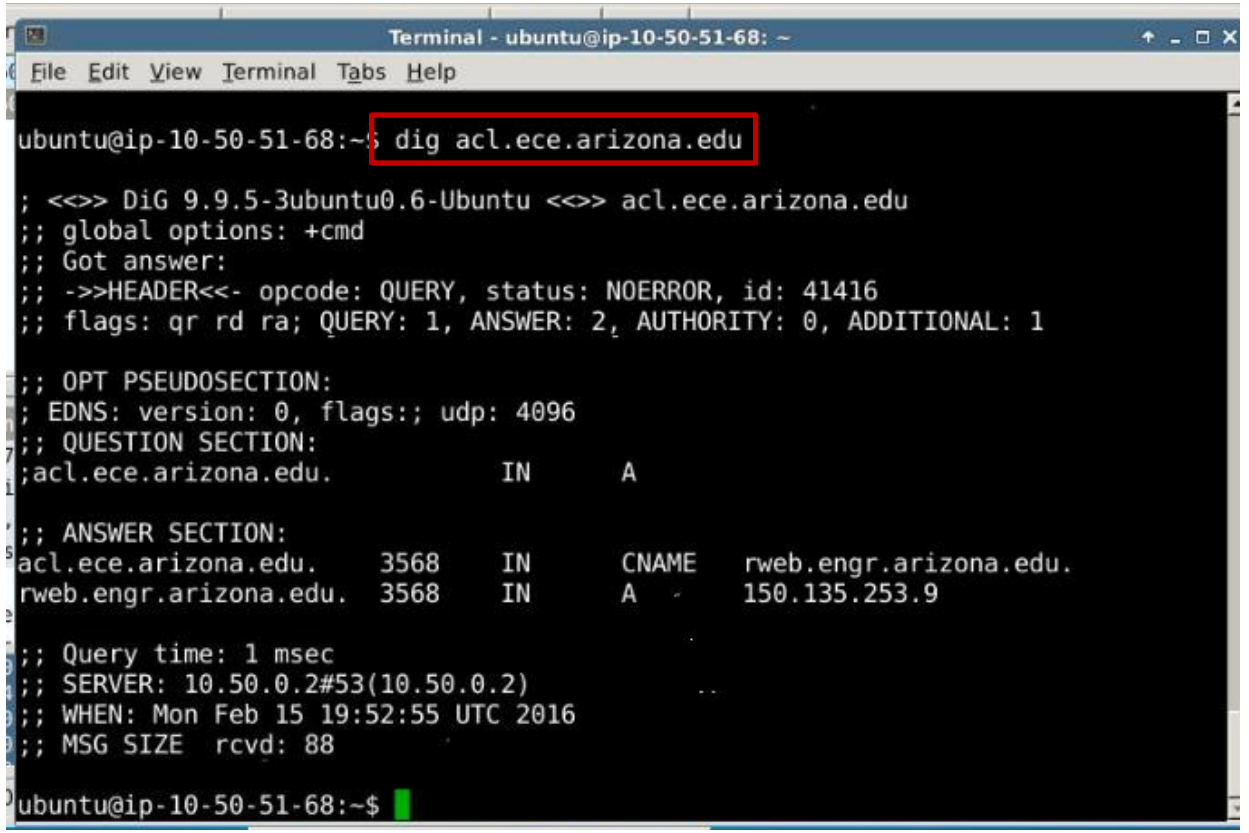
CAC Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Generate DNS traffic
  - From the terminal on the Server VM, type the following to generate DNS traffic:

```
dig acl.ece.arizona.edu
```



Experiment Instructions

- Step 2: Observe the UDP packets on Wireshark.
  - Go back to Wireshark and type on the filter field:

```
udp
```

  - Go through the packets in the list and observe the following:
    - Source and destination IPs
    - Source and destination port numbers on both the client and server
    - The packet parameters
    - Maximum and minimum values of these parameters

Experiment Instructions

- Step 3: Observe the DNS packets on Wireshark.
  - Go back to Wireshark and type on the filter field:

```
dns
```

  - Examine the listed packets and find the following information:
    - DNS headers
    - Maximum and minimum values of these headers
    - The listed queries and answers

Experiment Instructions

- Step 4: Generate more DNS packets
  - Look up at least four domain names with the dig command on a terminal in the Server VM
  - Go back to Wireshark and examine the DNS packets you created. Add the following to your lab report:
    - What information does a DNS request packet contain?
    - What information does a DNS reply packet contain?
    - Which resource is handling each DNS request for each domain name?
    - How many steps are required to obtain an IP address for each request?

Experiment Summary

- **Please note**
  - The UDP protocol is connectionless
  - DNS is a UDP protocol
  - The DNS protocol can have a variety of data sources, including authoritative name servers and resolvers

Lab Report

- List source and destination IPs and port numbers from the captured UDP packets
- List UDP packet parameters and maximum/minimum values
- List DNS headers and their values (include max/min values)
- List DNS queries and answers from captured packets

- What information does a DNS request packet contain?
- What information does a DNS reply packet contain?
- Which resource is handling each DNS request for each domain name?
- How many steps are required to obtain an IP address for each request?

Conclusion

- Wireshark is a very powerful tool that can have a variety of uses in computer and network security.
- In this lab, we barely scratched the surface of Wireshark's capabilities as a packet analyzer.
- We also experimented with different protocols and their structures.

AskCyPert

End of Lab

CAC Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION