Department of CEE/ Computer Science

Network Scanning

Beau Bikakis, Guang Jin Liu, Tue Le
Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

CSU Bakersfield
Chevron
Research Experience Vitalizing Science — University Program
NSF

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

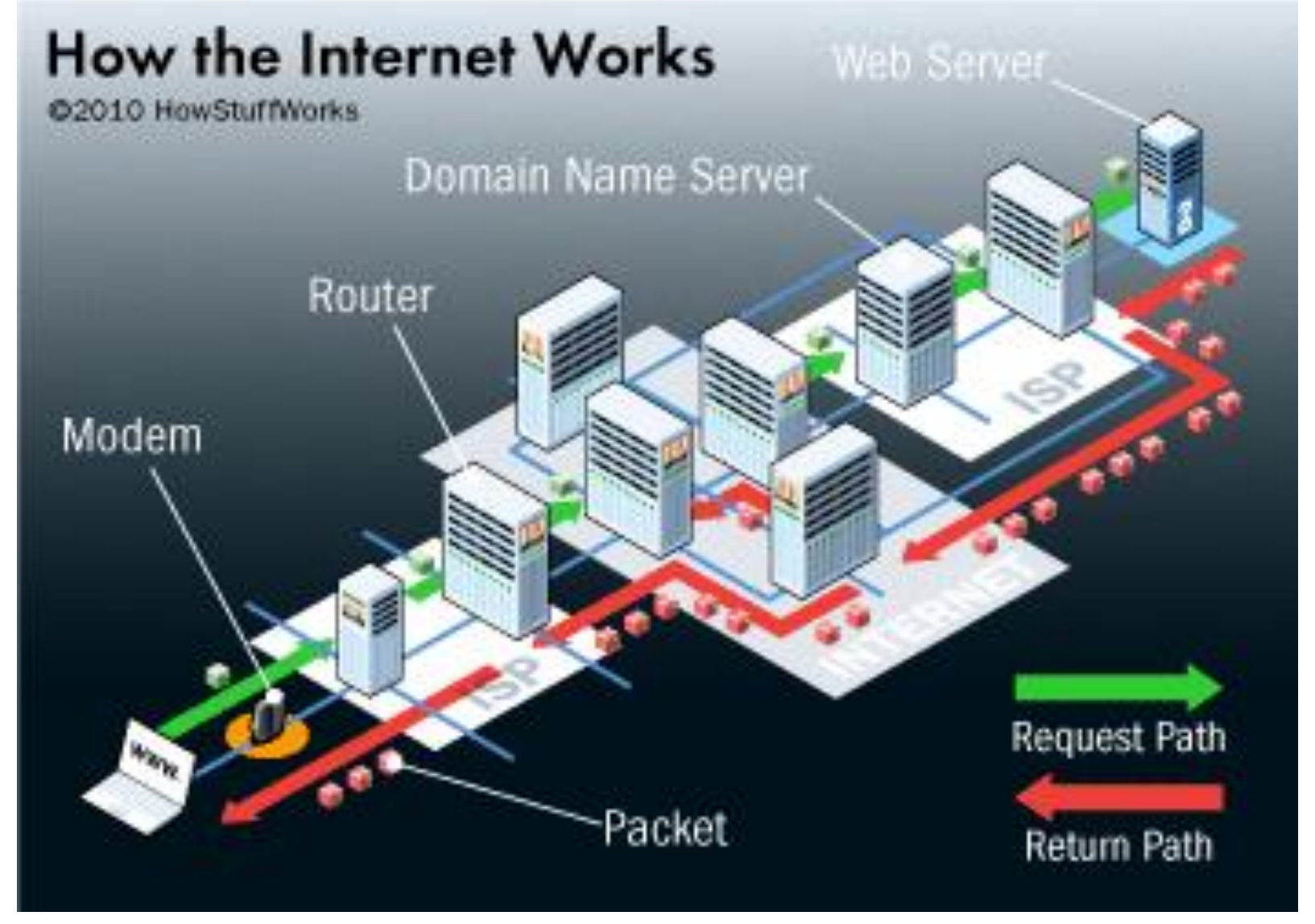
Background

How does the Internet work?

The Internet is the interaction of many connected devices across the world. It is a combination of hardware (computers, routers, servers, etc.) and protocols (a common set of rules for all internet devices to follow). All devices on the Internet can speak to each other because they all follow the same set of protocols (TCP/IP).

When a device is connected to the Internet through a local area network, it is given a special IP address to differentiate it from all the other devices that are also connected to the Internet. The IP address has two main functions: network identification and location addressing.

Client computers send requests to an Internet server in order to open web pages, watch videos, etc. The request goes through a series of routers to reach the Internet server, the server searches its database for data that matches the request and then sends back its response. The client is the input and the server is the output.



What is Network Scanning?

Network scanning is the use of scanning software to identify servers, devices, and clients on the network. It can be done by administrators looking to secure their network or hackers looking to exploit vulnerabilities.

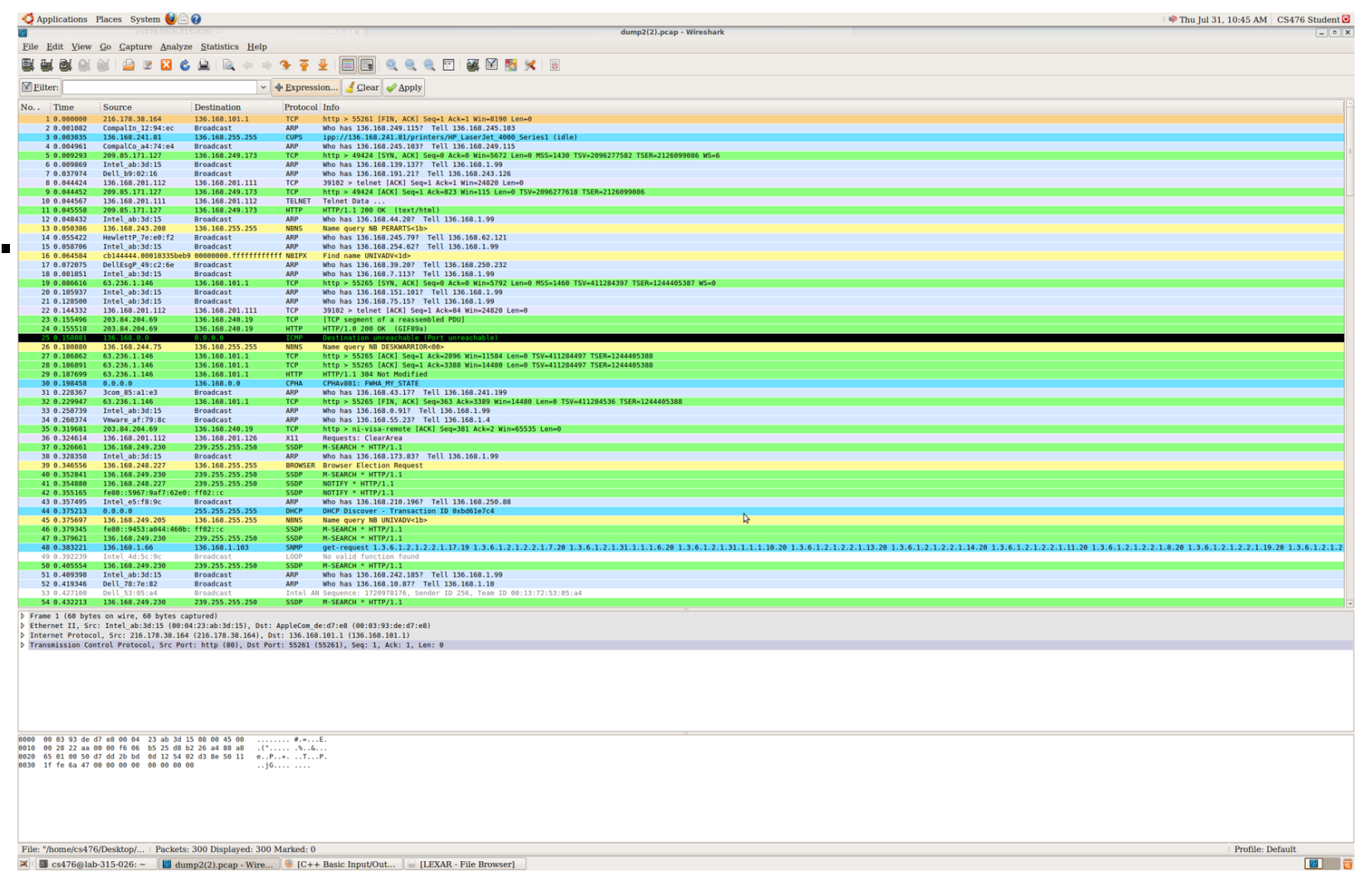
How does Network Scanning work?

By using the correct programs and knowing how to use them, scanning networks can become quiet easy. Those programs can scan network vulnerabilities, capture packets, and detect incoming threats. Keep this in mind when you are on the Internet as anyone can scan your web activity to quickly find unencrypted passwords and determine what websites you have been on.

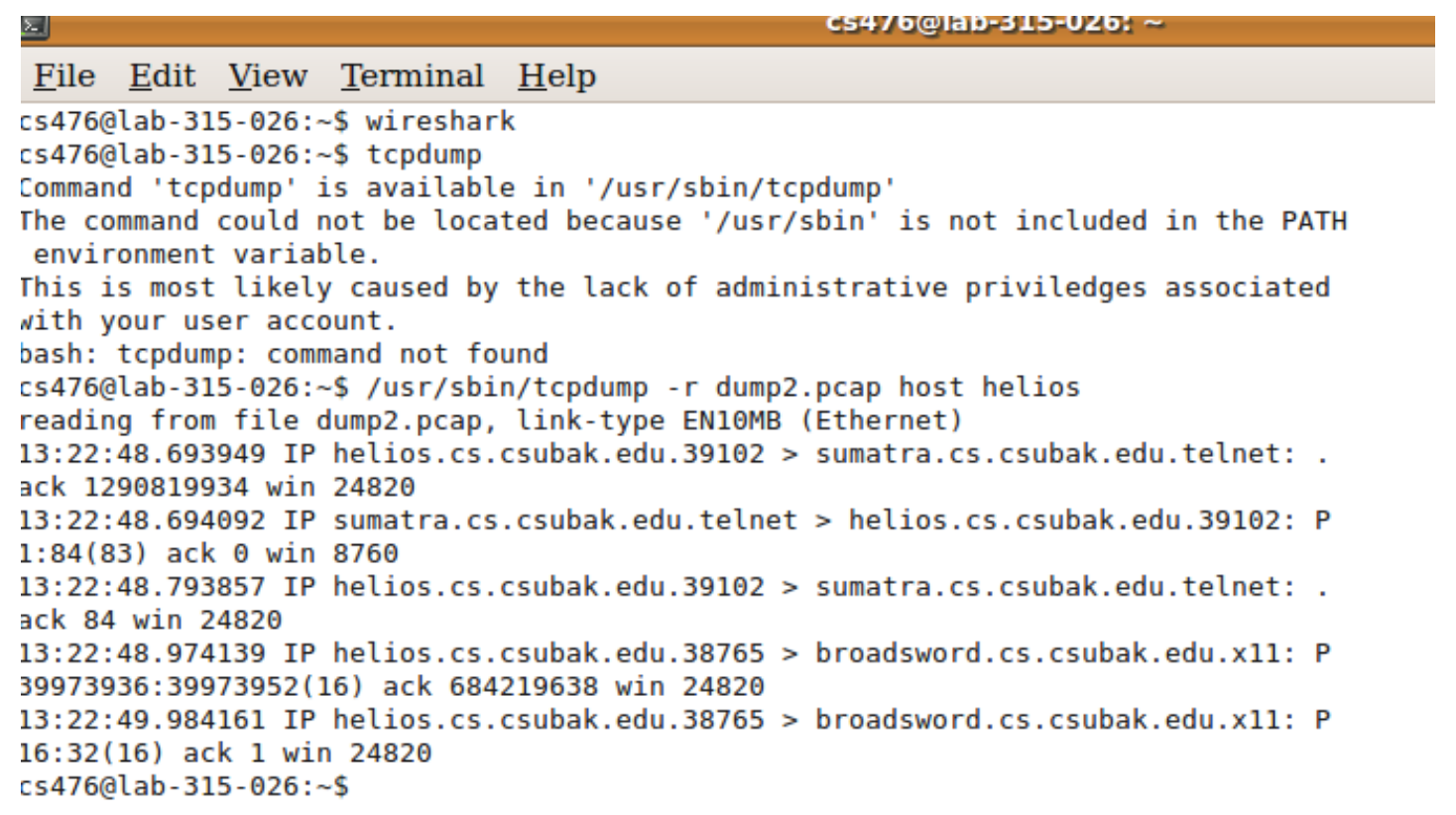
Network Scanning Programs

Wireshark

- Scans network traffic.
- Analyzes packets (data that can be transferred over a network).
- Filters through packets to find specific criteria.
- Is graphics-based instead of terminal-based.
- Monitor data coming in and out of your network.



TCPdump

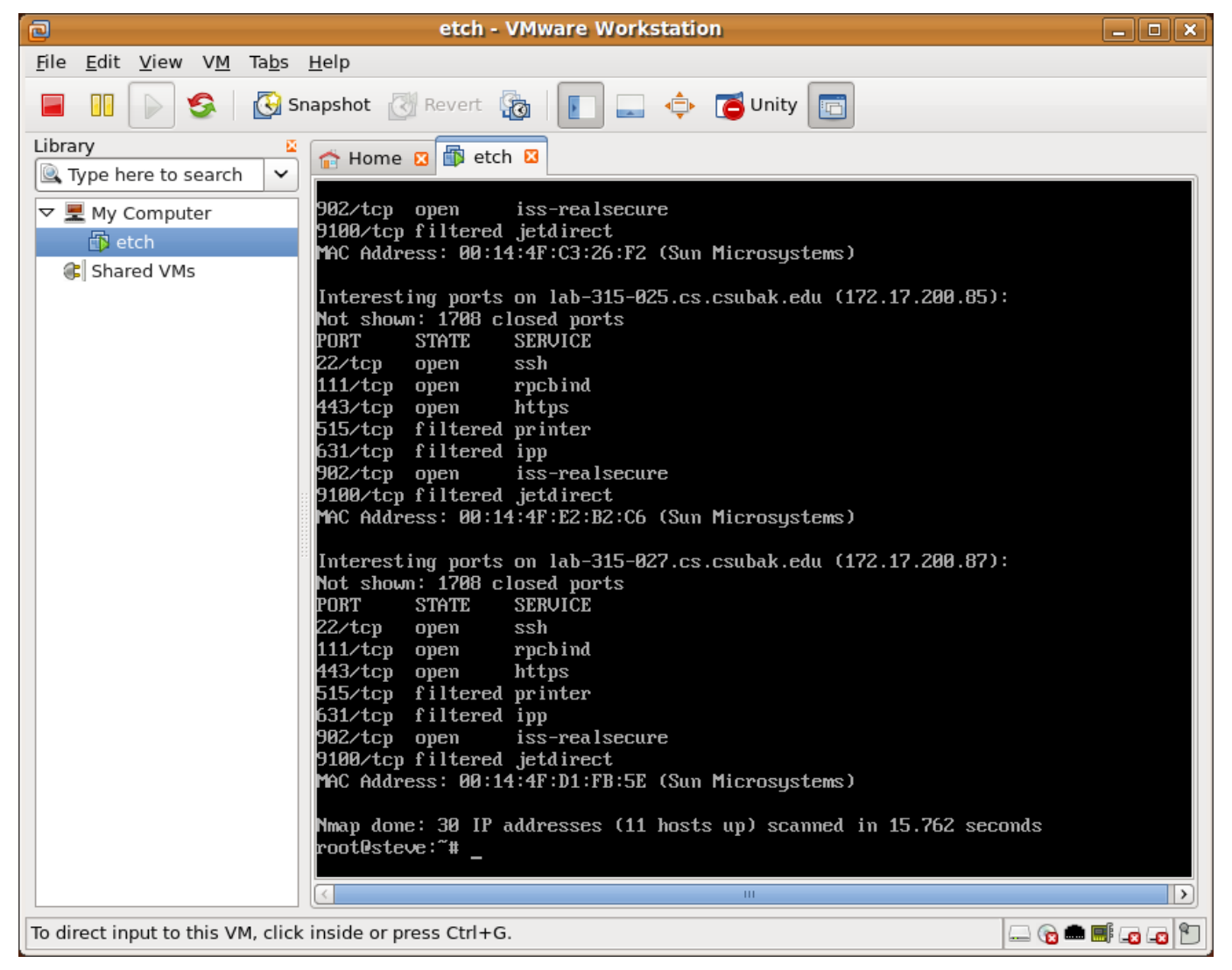


```
cs476@lab-315-026: ~
File  Edit  View  Terminal  Help
cs476@lab-315-026:~$ wireshark
cs476@lab-315-026:~$ tcpdump
Command 'tcpdump' is available in '/usr/sbin/tcpdump'
The command could not be located because '/usr/sbin' is not included in the PATH
 environment variable.
This is most likely caused by the lack of administrative priviledges associated
with your user account.
bash: tcpdump: command not found
cs476@lab-315-026:~$ /usr/sbin/tcpdump -r dump2.pcap host helios
reading from file dump2.pcap, link-type EN10MB (Ethernet)
13:22:48.693949 IP helios.cs.csubak.edu.39102 > sumatra.cs.csubak.edu.telnet: .
ack 1290819934 win 24820
13:22:48.694092 IP sumatra.cs.csubak.edu.telnet > helios.cs.csubak.edu.39102: P
1:84(83) ack 0 win 8760
13:22:48.793857 IP helios.cs.csubak.edu.39102 > sumatra.cs.csubak.edu.telnet: .
ack 84 win 24820
13:22:48.974139 IP helios.cs.csubak.edu.38765 > broadsword.cs.csubak.edu.x11: P
39973936:39973952(16) ack 684219638 win 24820
13:22:49.984161 IP helios.cs.csubak.edu.38765 > broadsword.cs.csubak.edu.x11: P
16:32(16) ack 1 win 24820
cs476@lab-315-026:~$
```

- Acts similar to Wireshark but has a different interface.
- Terminal-based.
- You type in command for which filter you want to apply.

Nmap

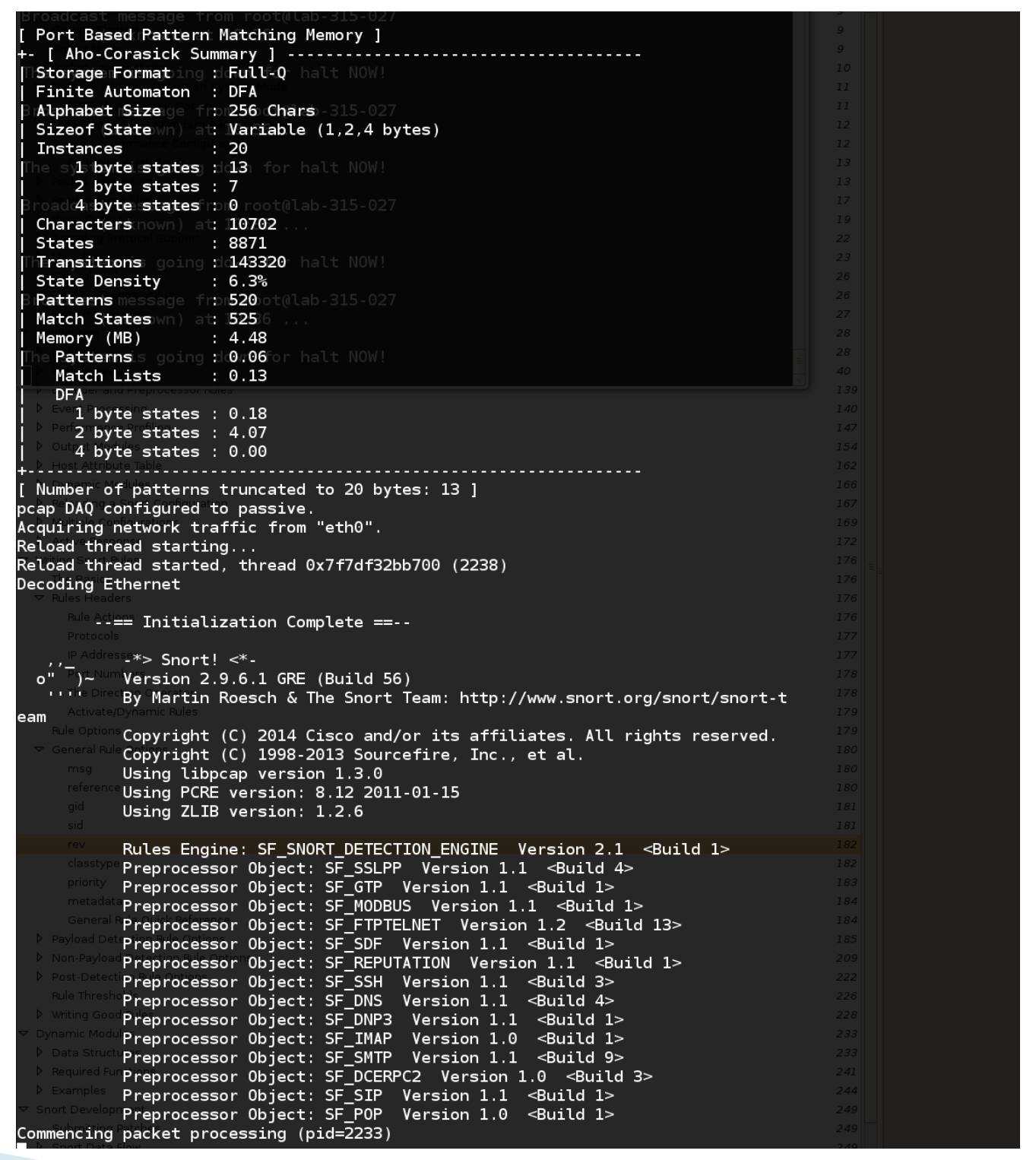
- Shows all hosts and devices connected to your network.
- Creates a virtual "map".
- Can determine the operating system of the target.
- Discovers hosts by sending a packet and analyzing the response.



```
902/tcp  open     iss-realsecure
9100/tcp filtered jetdirect
MAC Address: 00:14:4F:C3:26:F2 (Sun Microsystems)

Interesting ports on lab-315-025.cs.csubak.edu (172.17.200.85):
Not shown: 1708 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
111/tcp  open     rpcbind
443/tcp  open     https
515/tcp  filtered printer
631/tcp  filtered ipp
902/tcp  open     iss-realsecure
9100/tcp filtered jetdirect
MAC Address: 00:14:4F:E2:B2:C6 (Sun Microsystems)

Interesting ports on lab-315-027.cs.csubak.edu (172.17.200.87):
Not shown: 1708 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
111/tcp  open     rpcbind
443/tcp  open     https
515/tcp  filtered printer
631/tcp  filtered ipp
902/tcp  open     iss-realsecure
9100/tcp filtered jetdirect
MAC Address: 00:14:4F:D1:FB:5E (Sun Microsystems)

Nmap done: 30 IP addresses (11 hosts up) scanned in 15.762 seconds
root@steve:~# _
```

To direct input to this VM, click inside or press Ctrl+G.

Snort



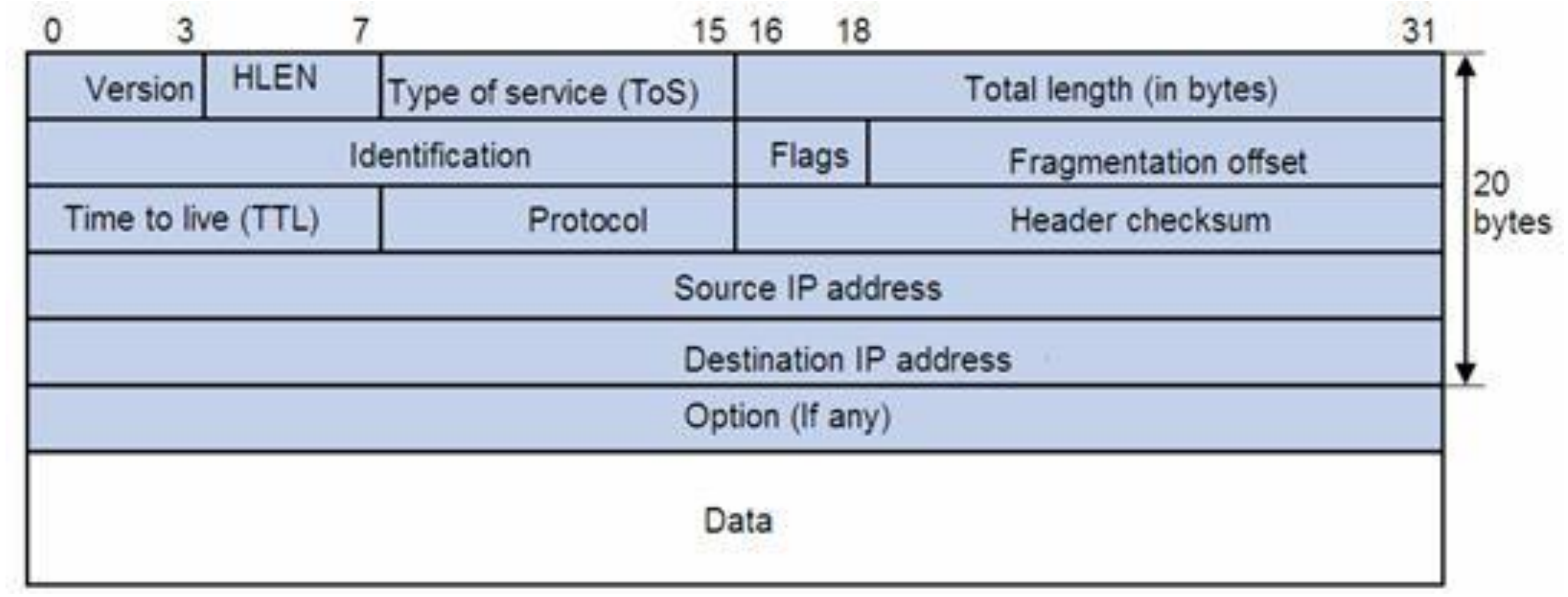
```
[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -------------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 20
|     1 byte states : 13
|     2 byte states : 7
|     4 byte states : 0
| Characters        : 10702
| States            : 8871
| Transitions       : 143320
| State Density     : 6.3%
| Patterns          : 520
| Match States      : 525
| Memory (MB)       : 4.48
|   Patterns        : 0.06
|   Match Lists     : 0.13
|   DFA
|     1 byte states : 0.18
|     2 byte states : 4.07
|     4 byte states : 0.00
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 13 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Reload thread starting...
Reload thread started, thread 0x7f7df32bb700 (2238)
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.1 GRE (Build 56)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.3.0
           Using PCRE version: 8.12 2011-01-15
           Using ZLIB version: 1.2.6

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
Commencing packet processing (pid=2233)
```

- Detect the intrusion of computers from outside world.
- Detect the intrusion in and out from the computer.
- Can choose between different types of alerts and actions for different inputs.
- Has three settings: sniffer, packet logger, and Network intrusion detection.

About the Network

Network

- Network is a subnet of links that get data to destination IP
- A Network is two or more computers linked together in order to share resources
- Data is organized into packets.
- There are series of headers for the different tasks within the packet.
- Host to network is physical connection between two machines, such as WiFi, Ethernet, etc.



<table>
<tr><td>Version</td><td>HLEN</td><td>Type of service (ToS)</td><td colspan="2">Total length (in bytes)</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragmentation offset</td></tr>
<tr><td colspan="2">Time to live (TTL)</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Option (If any)</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Network Vulnerabilities

- Bugs in server programs, client programs, websites or web programs.
  - Mistake in program code.
  - Exploitable feature of program.
  - Malicious code.
- No default encryption that protects from packet sniffing.
- No verification of addresses and infrastructure servers.

Additional Info.

- Most programs shown here are totally free to download.
- It is illegal to scan other people's network without proper clearance.
- Permission is needed to scan other people's network.

References

Wireshark:	http://www.wireshark.org/
TCPdump:	http://www.tcpdump.org/
Nmap:	http://nmap.org/
Snort:	https://www.snort.org/
IP protocol:	https://www.ietf.org/rfc/rfc791.txt