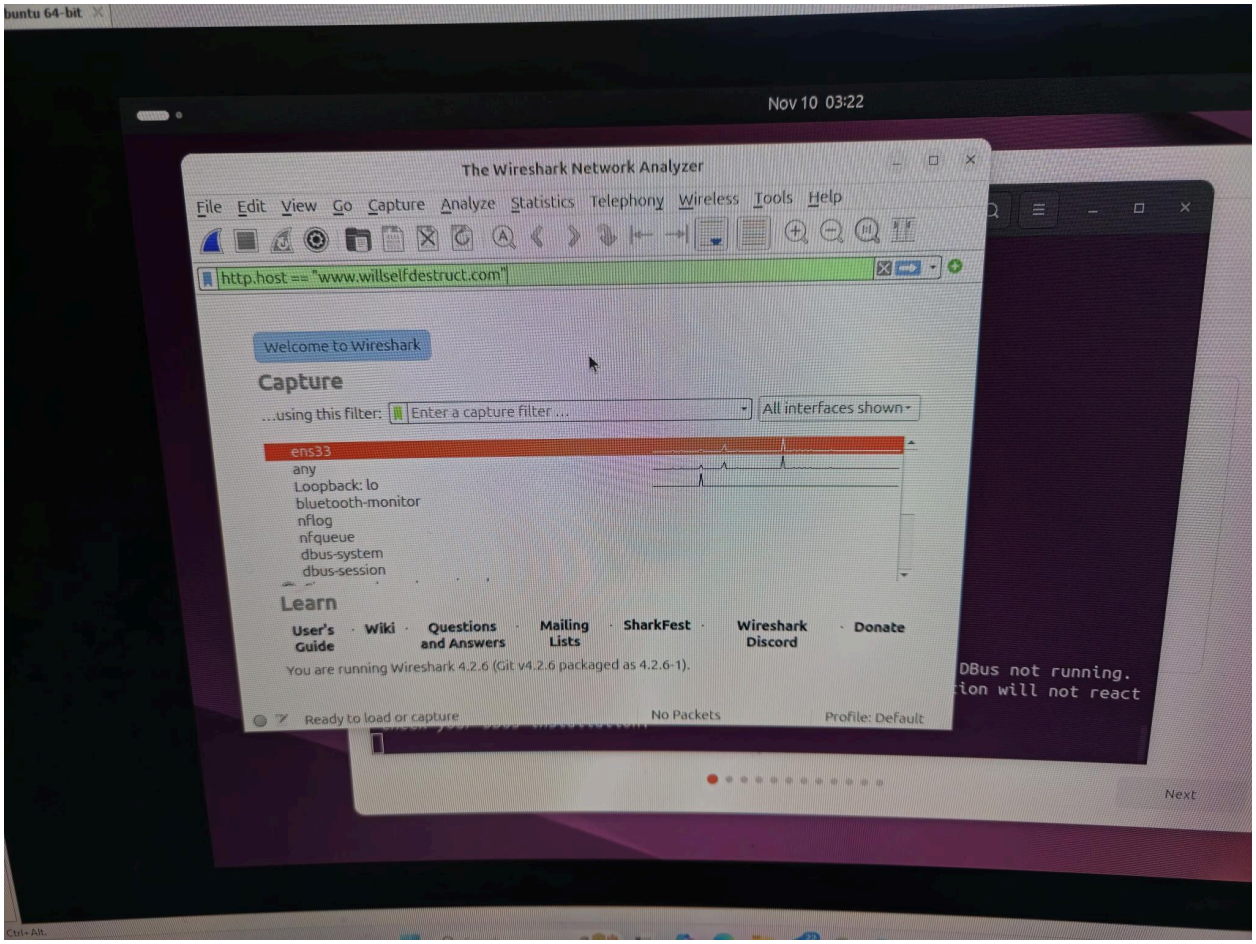
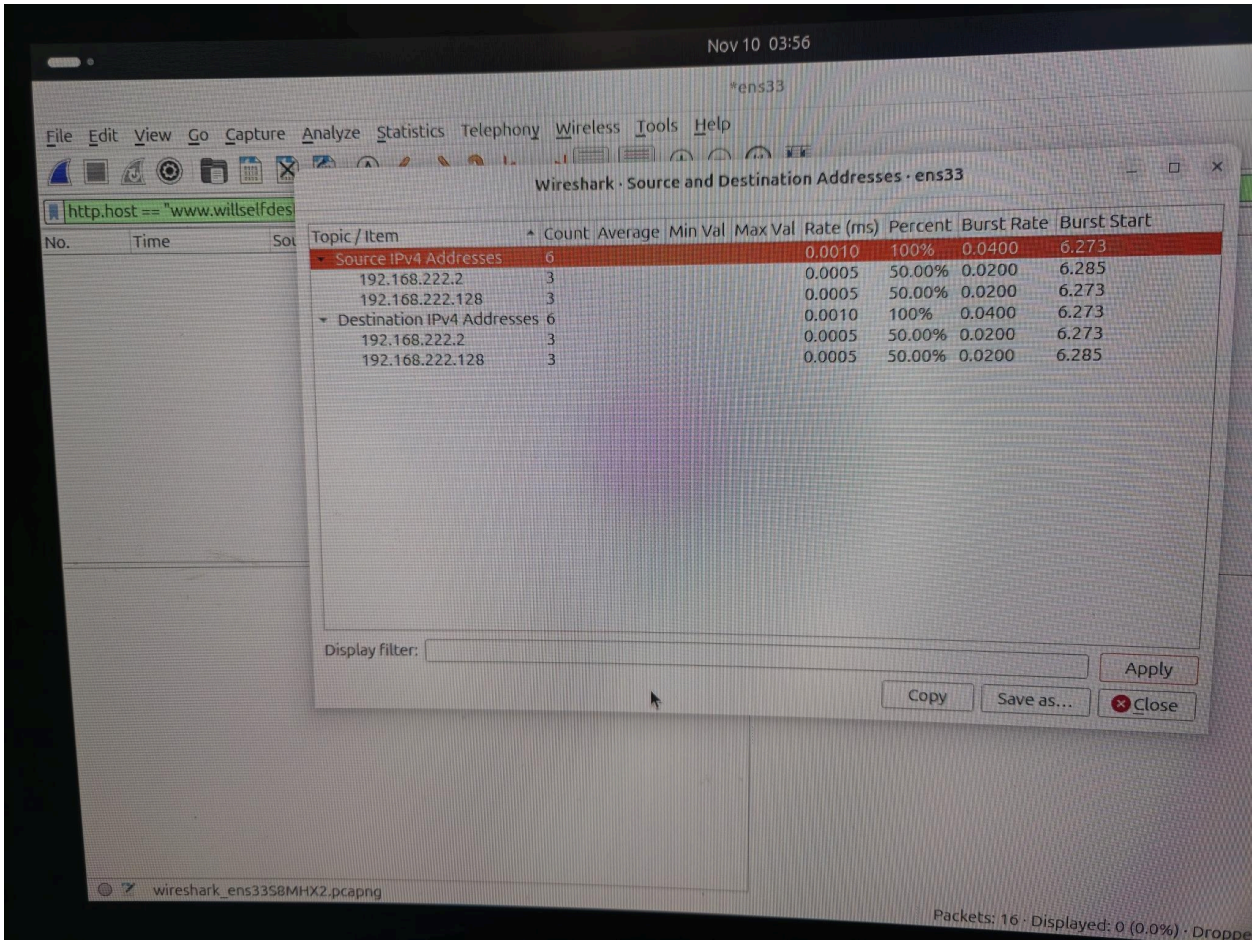
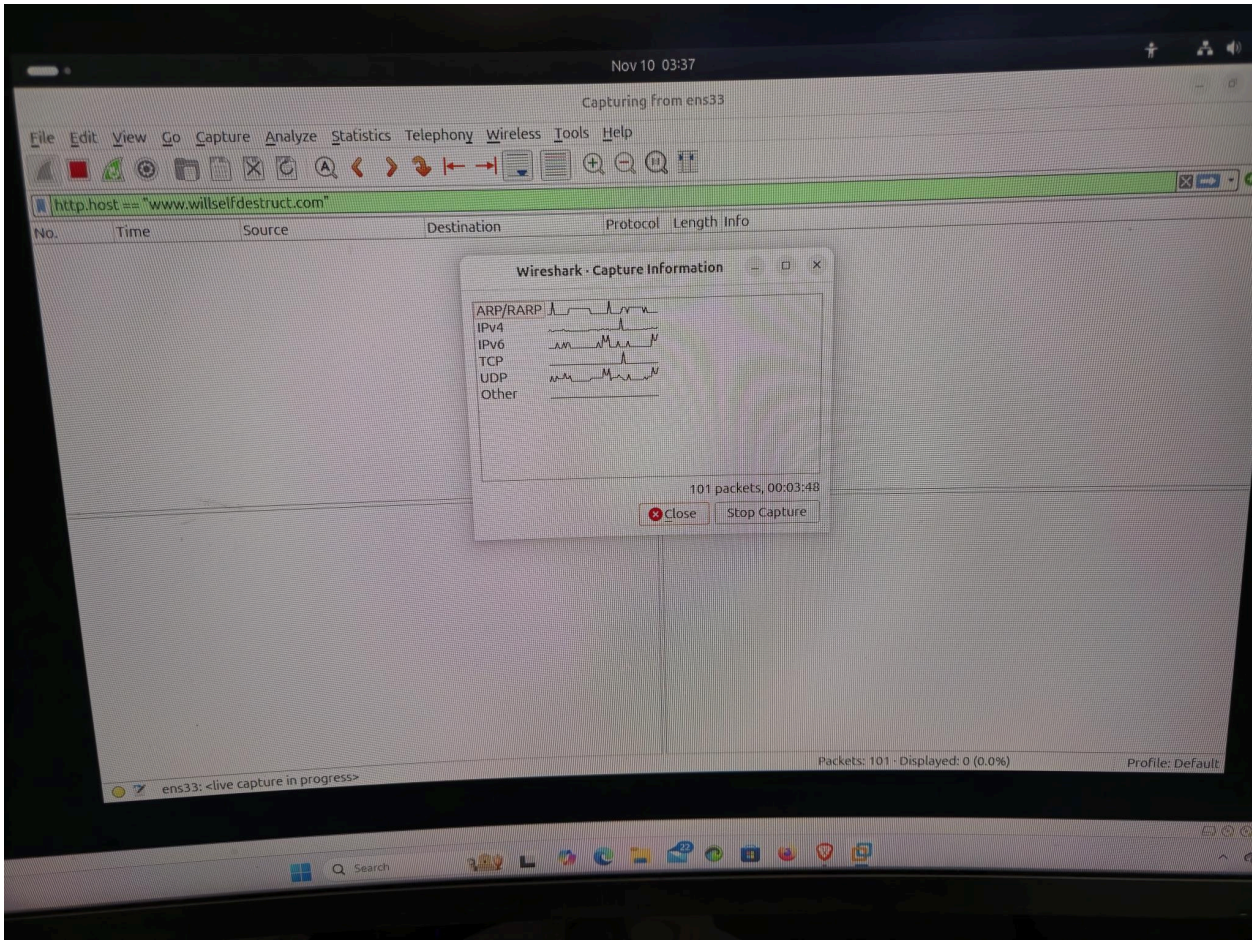
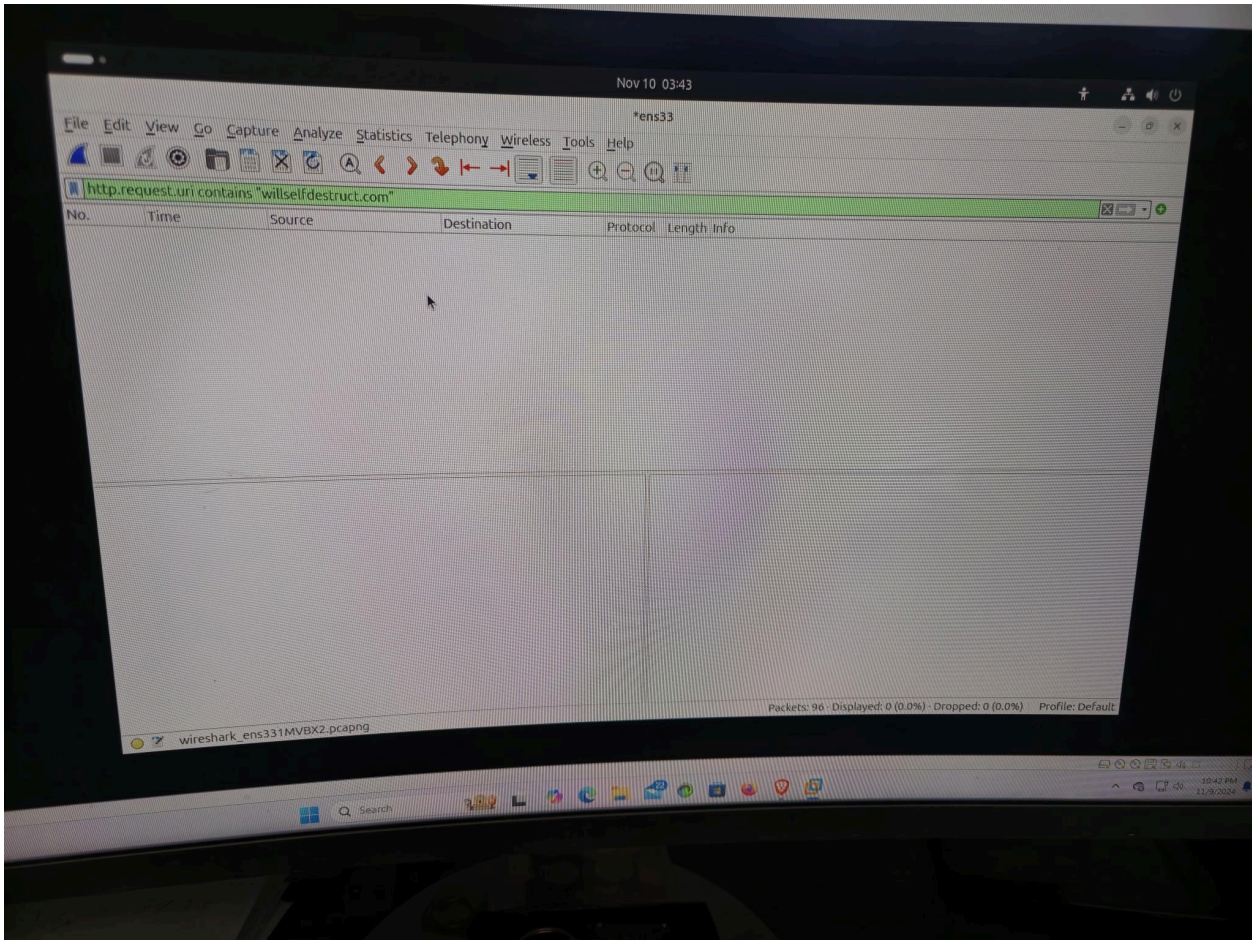
Branden Solomon
Professor Anthony
11/9/24
CTEC 350

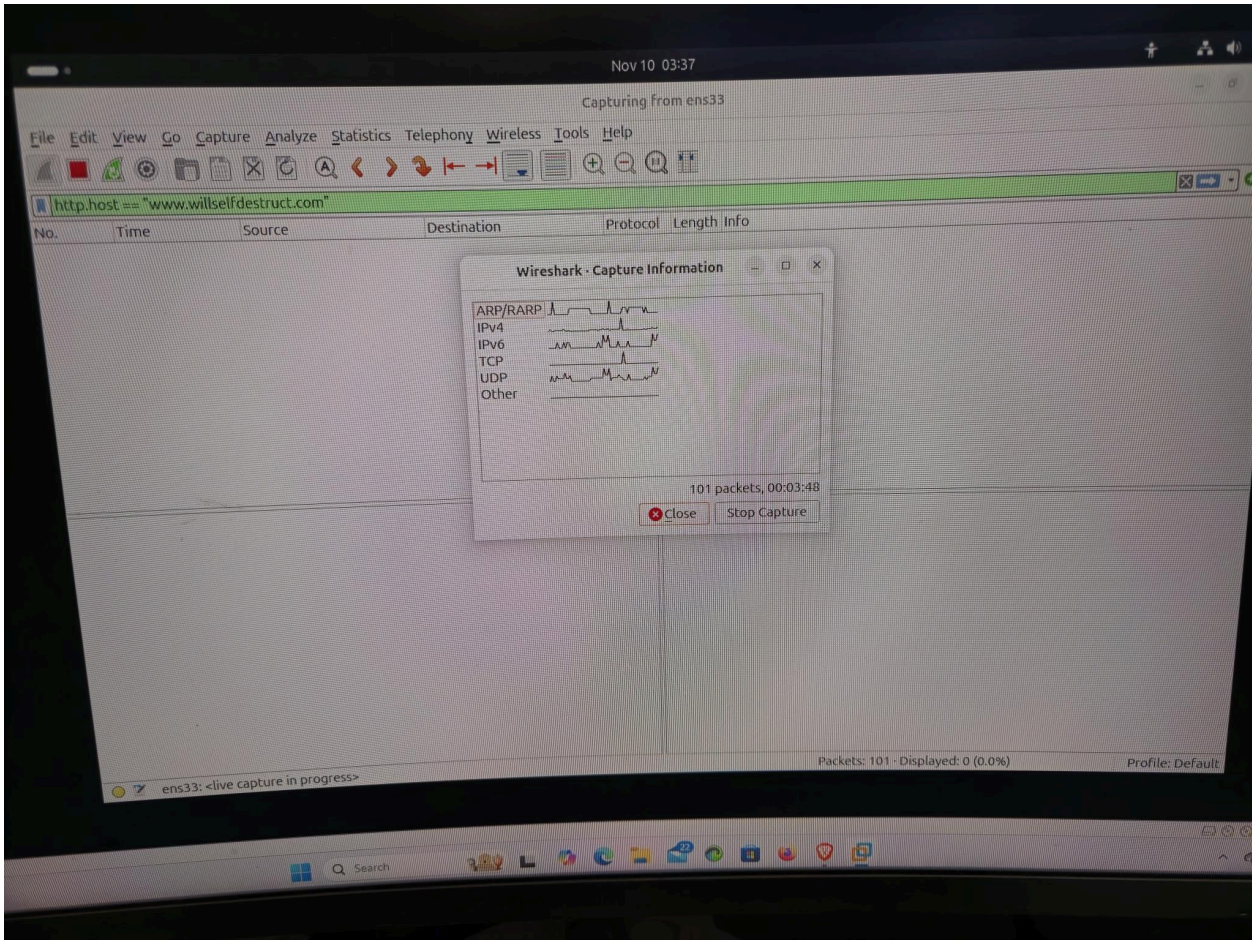
Project Wireshark

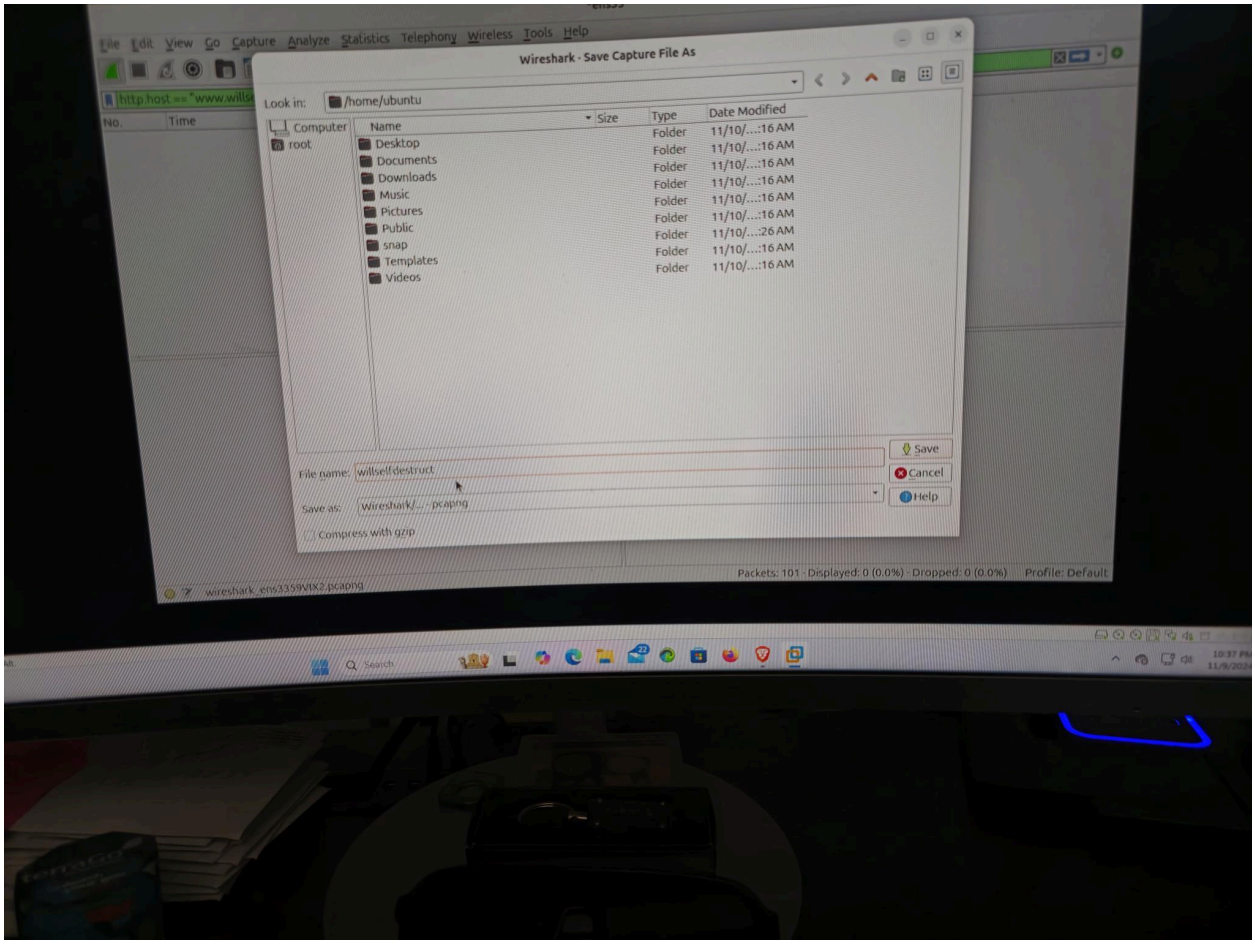
1. 
buntu 64-bit
Nov 10 03:22
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host == "www.willselfdestruct.com"
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
ens33
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.6 (Git v4.2.6 packaged as 4.2.6-1).
Ready to load or capture
No Packets
Profile: Default
DBus not running.
ion will not react
Next
Ctrl+Alt

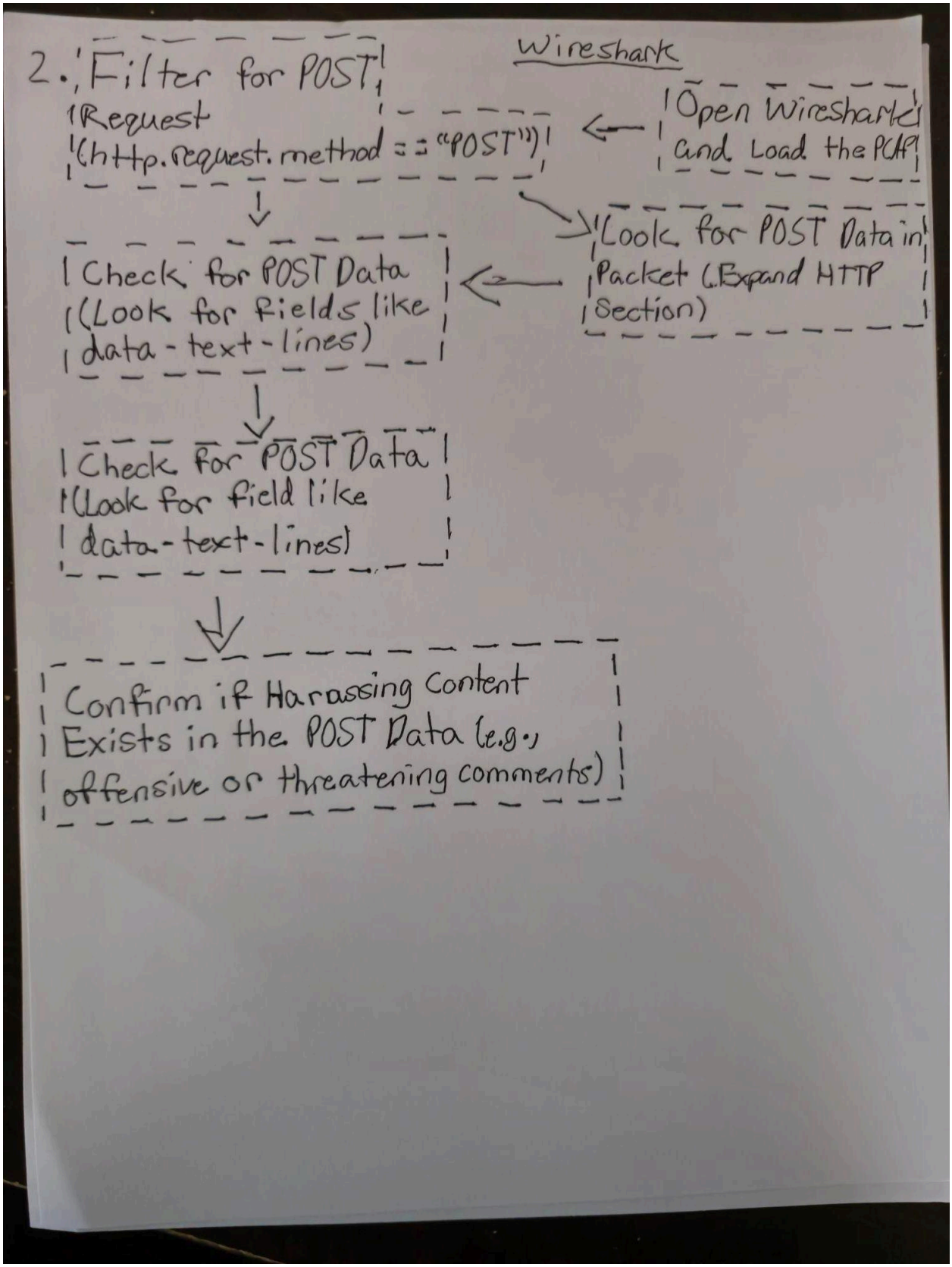

Nov 10 03:56
*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host == "www.willselfdes
No. Time
Wireshark · Source and Destination Addresses · ens33
Topic / Item Count Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
Source IPv4 Addresses 6 0.0010 100% 0.0400 6.273
192.168.222.2 3 0.0005 50.00% 0.0200 6.285
192.168.222.128 3 0.0005 50.00% 0.0200 6.273
Destination IPv4 Addresses 6 0.0010 100% 0.0400 6.273
192.168.222.2 3 0.0005 50.00% 0.0200 6.273
192.168.222.128 3 0.0005 50.00% 0.0200 6.285
Display filter:
Apply
Copy
Save as...
Close
wireshark_ens33S8MHX2.pcapng
Packets: 16 · Displayed: 0 (0.0%) · Droppe


Nov 10 03:37
Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host == "www.willselfdestruct.com"
No. Time Source Destination Protocol Length Info
Wireshark · Capture Information
ARP/RARP
IPv4
IPv6
TCP
UDP
Other
101 packets, 00:03:48
Close
Stop Capture
ens33: <live capture in progress>
Packets: 101 · Displayed: 0 (0.0%)
Profile: Default
Search


Nov 10 03:43
*ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.uri contains "willselfdestruct.com"
No. Time Source Destination Protocol Length Info
Packets: 96 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%) Profile: Default
wireshark_ens331MVBX2.pcapng
Search


Nov 10 03:37
Capturing from ens33
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.host == "www.willselfdestruct.com"
No. Time Source Destination Protocol Length Info
Wireshark · Capture Information
ARP/RARP
IPv4
IPv6
TCP
UDP
Other
101 packets, 00:03:48
Close
Stop Capture
ens33: <live capture in progress>
Packets: 101 · Displayed: 0 (0.0%)
Profile: Default
Search


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Save Capture File As
Look in: /home/ubuntu
Computer
root
Name
Size
Type
Date Modified
Desktop
Documents
Downloads
Music
Pictures
Public
snap
Templates
Videos
Folder
11/10/...:16 AM
11/10/...:26 AM
File name: willselfdestruct
Save as: Wireshark/... pcapng
Compress with gzip
Save
Cancel
Help
Packets: 101 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
wireshark_ens3359VIX2.pcapng

2. 

The POST request contains harassing comments like offensive language or threats.

3. The IP address or MAC address corresponds to a suspect on the class roster. Let’s say it’s Jeremy Ledvkin.
4. The MAC address found in the packet corresponds to Jeremy Ledvkin's device.
5. The POST request timestamp shows the suspect accessed the website on July 15, 2024, at 2:32 PM UTC.