Activity 2
Network Traffic Investigation and Analysis

Be able to investigate captured network traffic data using various network analysis tools. Be able to follow properly the standard procedure in performing network traffic data investigation process. Use the activity template in providing the necessary screenshots.

Activity Resources
Evidence: CTAINASLNetCapture.pcap
Tools: Wireshark, NetworkMiner, VirusTotal (Online)

Activity Procedure(s)
Open Wireshark and load the network capture file (CTAINASLNetCapture.pcap). Perform the necessary network investigation of the captured network traffic by answering the following questions using various examination techniques (filtering, statistics analysis, and expert information analysis):

1. What is the IP Address of the infected machine?
2. Where did the machine obtain the malware infection?
3. Does the identified malware make some internet connection? What kind of connection does the malware activity suggests?

Submission Note (Individual Activity)
Use file name convention (LASTNAME_CTAINASL_SECTION_TERM_AY_Activity2.pdf).
Submit/upload Softcopy (PDF file) in MS Teams
Submit a PRINTED activity rubric.

ACTIVITY DOCUMENTATION

Group Name *Ctrl+Z* Wednesday, April 9, 2025

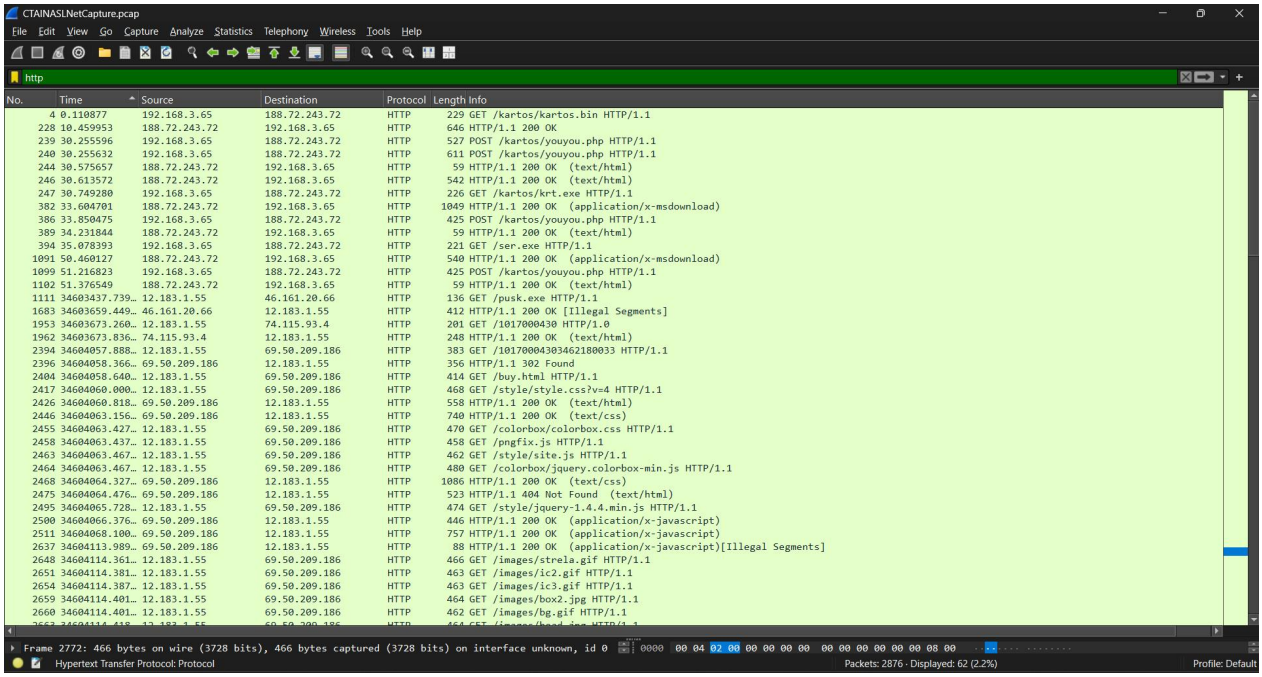
Members Surname, First Name MI. (Alphabetical)

1. *Cano, Kaide M.*
2. *Cuenca, Sophia T.*
3. *Dionela, Terrence A.*
4. *Umenaan, Darwin F.*
5. _____

Instruction(s): Provide the appropriate screenshot/screen capture of your workstation.

Wireshark Filtering

Display here the Wireshark HTTP filtered traffic report.



Observation and Findings: What does the captured network traffic (http) suggests? Does the traffic contain malicious contents? If yes, extract the content and conduct further analysis using VirusTotal (Online Tool).

The captured HTTP traffic strongly suggests malicious activity. Several suspicious files with .exe and .php extensions such as kartos.bin, krt.exe, sen.exe, and pusk.exe were downloaded or accessed by the machine at IP address 12.183.1.55. These are indicative of malware payloads.

Wireshark Statistics (IPv4 Statistics)
Display here the Wireshark IPv4 statistics summary report.

Wireshark · IPv4 Statistics / All Addresses · CTAINASLNetCapture.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	2876				0.0000	100%	0.4100	34603668.618
8.8.8.8	232				0.0000	8.07%	0.3000	34603667.841
8.8.4.4	66				0.0000	2.29%	0.0600	34603926.322
74.115.93.4	10				0.0000	0.35%	0.0400	34603673.837
69.50.209.225	12				0.0000	0.42%	0.0300	34603668.618
69.50.209.224	13				0.0000	0.45%	0.0300	34603668.717
69.50.209.223	13				0.0000	0.45%	0.0300	34603668.569
69.50.209.188	12				0.0000	0.42%	0.0300	34603668.538
69.50.209.186	504				0.0000	17.52%	0.1800	34604114.360
69.50.209.185	13				0.0000	0.45%	0.0300	34603668.667
69.50.209.184	12				0.0000	0.42%	0.0300	34603668.777
69.50.209.183	13				0.0000	0.45%	0.0300	34603668.618
69.50.209.182	12				0.0000	0.42%	0.0300	34603668.767
69.50.209.149	13				0.0000	0.45%	0.0300	34603668.558
69.50.209.148	12				0.0000	0.42%	0.0300	34603668.618
69.50.209.140	12				0.0000	0.42%	0.0300	34603668.527
69.50.209.139	13				0.0000	0.45%	0.0300	34603668.618
69.197.161.205	12				0.0000	0.42%	0.0300	34603668.657
69.197.161.204	12				0.0000	0.42%	0.0300	34603668.667
69.197.161.203	12				0.0000	0.42%	0.0300	34603668.707
69.197.161.202	12				0.0000	0.42%	0.0300	34603668.707
46.161.20.66	580				0.0000	20.17%	0.0600	34603659.377

Display filter: Enter a display filter ... Apply

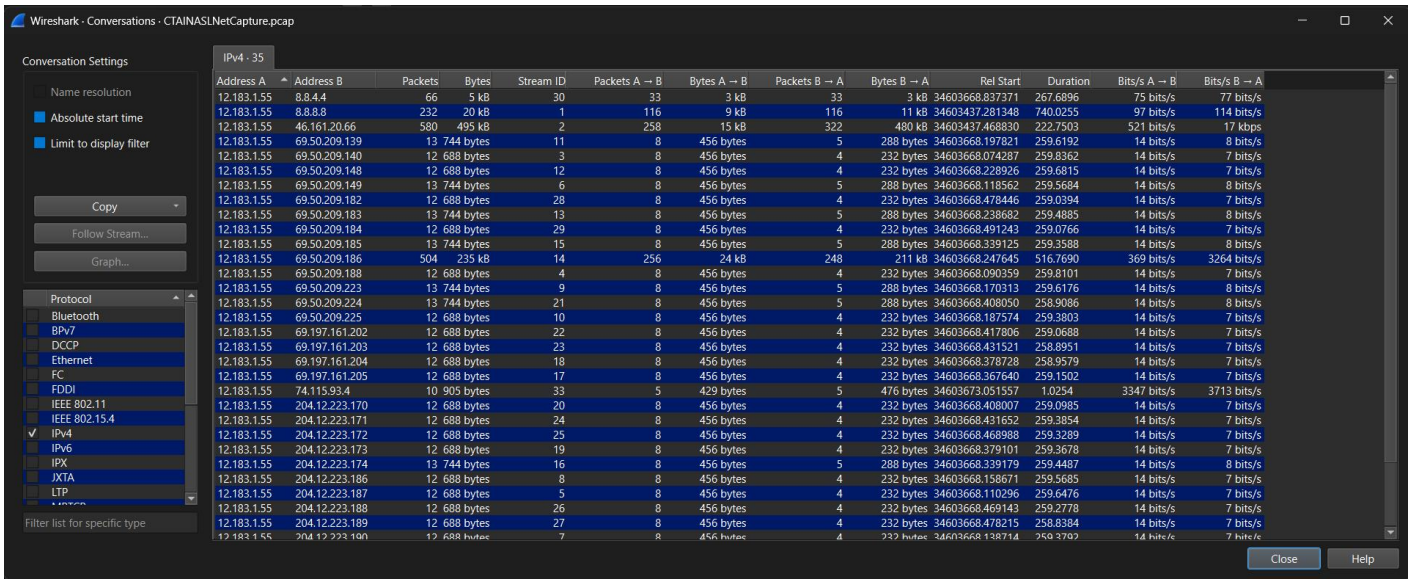
Copy Save as... Close

Observation and Findings: What does the statistics (IPv4 Addresses) suggests? Explain!

This shows a potentially abnormal concentration of traffic to a few non-public, suspicious-looking IPs. And it could be a legit application communicating with external servers or malware or spyware activity, especially if the traffic is outbound

Wireshark Statistics (Conversations)

Display here the Wireshark Conversations statistics summary report.

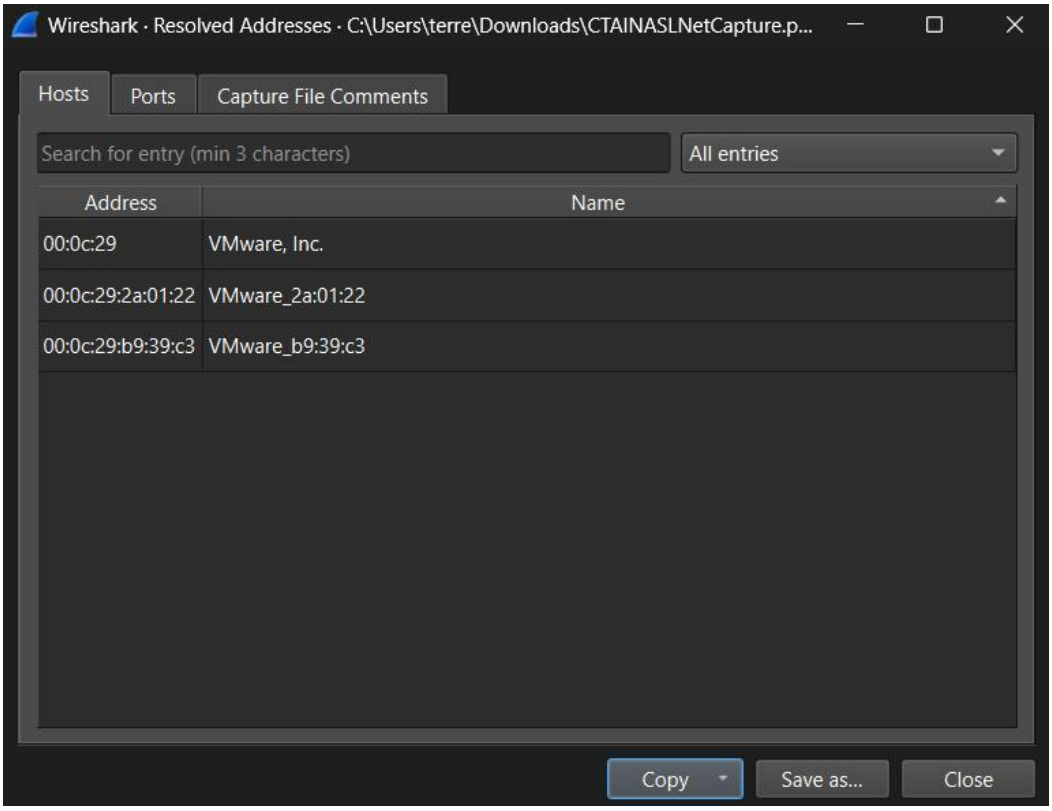


Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
12.183.1.55	8.8.4.4	66	5 kB	30	33	3 kB	33	3 kB	34603668.837371	267.6896	75 bits/s	77 bits/s
12.183.1.55	8.8.8.8	232	20 kB	1	116	9 kB	116	11 kB	34603437.281348	740.0255	97 bits/s	114 bits/s
12.183.1.55	46.161.20.66	580	495 kB	2	258	15 kB	322	480 kB	34603437.468830	222.7503	521 bits/s	17 kbps
12.183.1.55	69.50.209.139	13	744 bytes	11	8	456 bytes	5	288 bytes	34603668.197821	259.6192	14 bits/s	8 bits/s
12.183.1.55	69.50.209.140	12	688 bytes	3	8	456 bytes	4	232 bytes	34603668.074287	259.8362	14 bits/s	7 bits/s
12.183.1.55	69.50.209.148	12	688 bytes	12	8	456 bytes	4	232 bytes	34603668.228926	259.6815	14 bits/s	7 bits/s
12.183.1.55	69.50.209.149	13	744 bytes	6	8	456 bytes	5	288 bytes	34603668.118562	259.5684	14 bits/s	8 bits/s
12.183.1.55	69.50.209.182	12	688 bytes	28	8	456 bytes	4	232 bytes	34603668.478446	259.0394	14 bits/s	7 bits/s
12.183.1.55	69.50.209.183	13	744 bytes	13	8	456 bytes	5	288 bytes	34603668.238682	259.4885	14 bits/s	8 bits/s
12.183.1.55	69.50.209.184	12	688 bytes	29	8	456 bytes	4	232 bytes	34603668.491243	259.0766	14 bits/s	7 bits/s
12.183.1.55	69.50.209.185	13	744 bytes	15	8	456 bytes	5	288 bytes	34603668.339125	259.3588	14 bits/s	8 bits/s
12.183.1.55	69.50.209.186	504	235 kB	14	256	24 kB	248	211 kB	34603668.247645	516.7690	369 bits/s	3264 bits/s
12.183.1.55	69.50.209.188	12	688 bytes	4	8	456 bytes	4	232 bytes	34603668.090359	259.8101	14 bits/s	7 bits/s
12.183.1.55	69.50.209.223	13	744 bytes	9	8	456 bytes	5	288 bytes	34603668.170313	259.6176	14 bits/s	8 bits/s
12.183.1.55	69.50.209.224	13	744 bytes	21	8	456 bytes	5	288 bytes	34603668.408050	258.9086	14 bits/s	8 bits/s
12.183.1.55	69.50.209.225	12	688 bytes	10	8	456 bytes	4	232 bytes	34603668.187574	259.3803	14 bits/s	7 bits/s
12.183.1.55	69.197.161.202	12	688 bytes	22	8	456 bytes	4	232 bytes	34603668.417806	259.0688	14 bits/s	7 bits/s
12.183.1.55	69.197.161.203	12	688 bytes	23	8	456 bytes	4	232 bytes	34603668.431521	258.8951	14 bits/s	7 bits/s
12.183.1.55	69.197.161.204	12	688 bytes	18	8	456 bytes	4	232 bytes	34603668.378728	258.9579	14 bits/s	7 bits/s
12.183.1.55	69.197.161.205	12	688 bytes	17	8	456 bytes	4	232 bytes	34603668.367640	259.1502	14 bits/s	7 bits/s
12.183.1.55	74.115.93.4	10	905 bytes	33	5	429 bytes	5	476 bytes	34603673.051557	1.0254	3347 bits/s	3713 bits/s
12.183.1.55	204.12.223.170	12	688 bytes	20	8	456 bytes	4	232 bytes	34603668.408007	259.0985	14 bits/s	7 bits/s
12.183.1.55	204.12.223.171	12	688 bytes	24	8	456 bytes	4	232 bytes	34603668.431652	259.3854	14 bits/s	7 bits/s
12.183.1.55	204.12.223.172	12	688 bytes	25	8	456 bytes	4	232 bytes	34603668.468988	259.3289	14 bits/s	7 bits/s
12.183.1.55	204.12.223.173	12	688 bytes	19	8	456 bytes	4	232 bytes	34603668.379101	259.3678	14 bits/s	7 bits/s
12.183.1.55	204.12.223.174	13	744 bytes	16	8	456 bytes	5	288 bytes	34603668.339179	259.4487	14 bits/s	8 bits/s
12.183.1.55	204.12.223.186	12	688 bytes	8	8	456 bytes	4	232 bytes	34603668.158671	259.5685	14 bits/s	7 bits/s
12.183.1.55	204.12.223.187	12	688 bytes	5	8	456 bytes	4	232 bytes	34603668.110296	259.6476	14 bits/s	7 bits/s
12.183.1.55	204.12.223.188	12	688 bytes	26	8	456 bytes	4	232 bytes	34603668.469143	259.2778	14 bits/s	7 bits/s
12.183.1.55	204.12.223.189	12	688 bytes	27	8	456 bytes	4	232 bytes	34603668.478215	258.8384	14 bits/s	7 bits/s
12.183.1.55	204.12.223.190	12	688 bytes	7	8	456 bytes	4	232 bytes	34603668.138714	259.3792	14 bits/s	7 bits/s

Observation and Findings: What does the statistics (Conversations) suggests? Explain!

In this conversation statistics the infected host 12.183.1.55 is talking to 30+ IP addresses

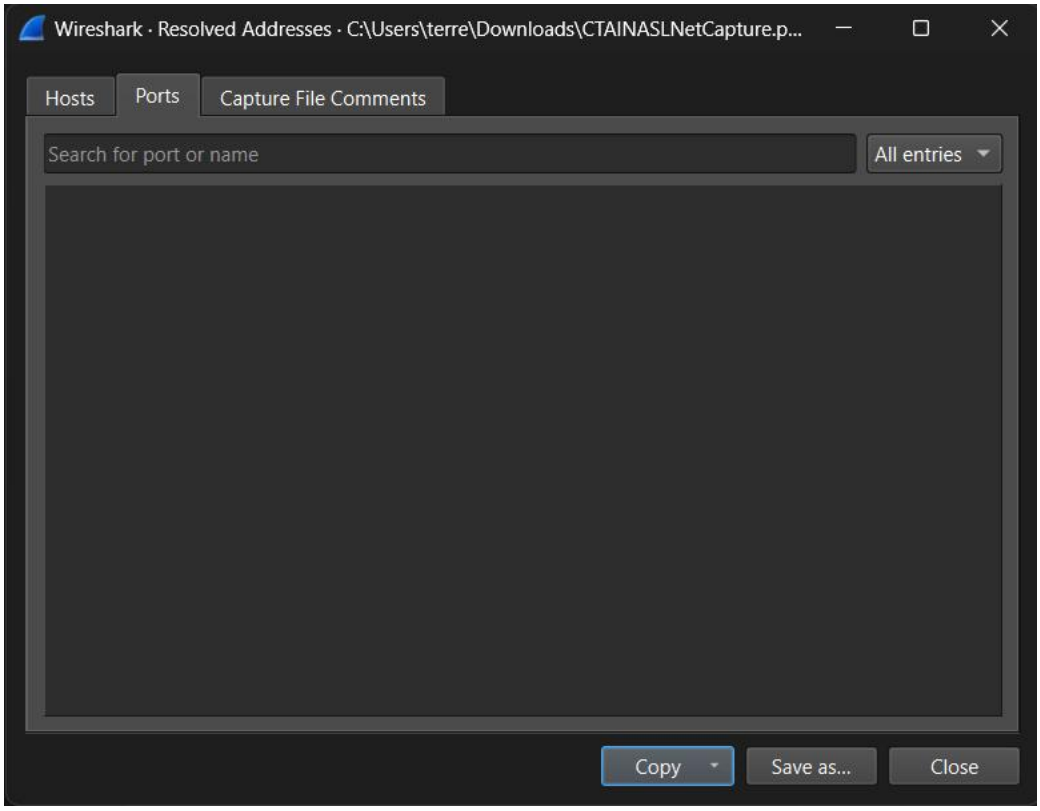
Wireshark Statistics (Resolved Host Addresses)
Display here the Wireshark Resolved Host Addresses statistics summary report.



Observation and Findings: What does the statistics (Resolved Hosts Addresses) suggests? Explain!

Suggests that the system running Wireshark is a VM, and possibly communicating with other VMs or using virtual interfaces.

Wireshark Statistics (Resolved Ports Addresses)
Display here the Wireshark Resolved Ports Addresses statistics summary report.



Observation and Findings: What does the statistics (Resolved Ports Addresses) suggests? Explain!

No ports were resolved

Question and Answer
Refer to the identified question(s) in the activity template.

What is the IP Address of the infected machine?

Answer: 12.183.1.55 Because This IP is consistently the source of communications in nearly all conversations

Where did the machine obtain the malware infection?

Answer: 46.161.20.66 This host shows a very large byte transfer (495 kB) to the infected machine (12.183.1.55). The direction of the data suggests the external server is sending a substantial payload this could be the malware being delivered.

Does the identified malware make some internet connection? What kind of connection does the malware activity suggests?

Answer: Yes (69.50.209.186), (204.12.223.186), Because this activity resembles Command and Control (C2) traffic, which is how malware communicates with its operator or controlling server.

NATIONAL UNIVERSITY
COLLEGE OF COMPUTING AND INFORMATION TECHNOLOGY

ACTIVITY RUBRICS

Group Name Ctrl+Z Wednesday, April 9, 2025

Members Surname, First Name MI. (Alphabetical)

1. Cano, Kaide M.
2. Cuenca, Sophia T.
3. Dionela, Terrence A.
4. Umenaan, Darwin F.
5. _____

Criteria	Activity Rubrics					Points
	Not Attempted (0 points)	Beginning (1 point)	Developing (2 points)	Proficient (3 points)	Exemplary (4 points)	
Use of Wireshark Tool	No attempt to use network analysis tool(s).	Incorrect or unsuitable tool(s) selected.	Tool(s) used is/are somewhat suitable but not optimal.	Selected appropriate tool(s) with minor mismatches to the scenario.	Selected the most appropriate tool(s) for the task based on evidence type and scenario.	
Use of Wireshark Filters	No attempt to perform filtering of network traffic data.	Filters not used or configured incorrectly, leading to large irrelevant data.	Basic filters applied; excessive or irrelevant data captured.	Capture filters set up correctly with minor inefficiencies.	Capture filters configured accurately; unnecessary data excluded effectively.	
Use of Wireshark Features	No attempt to use Wireshark features.	Wireshark features not used effectively; manual analysis dominates.	Limited use of Wireshark features; investigation hindered by inefficiency.	Basic features used effectively; advanced features used with some errors.	Advanced features used effectively (e.g., filters, color coding, statistics)	
Protocol Analysis	Protocol analysis not attempted.	Protocol analysis incorrect.	Basic protocol analysis performed; significant details overlooked.	Most protocols analyzed correctly; minor details missed.	Protocols analyzed thoroughly; key details (e.g., headers, flags, payloads) identified and explained.	
Documentation	No attempt to provide report documentation of findings.	Poor documentation of findings; lacks structure or critical details.	Basic report provided with significant omissions or unclear explanations.	Detailed report provided; minor gaps in methods or findings.	Comprehensive report including methods, findings, and recommendations.	

Total Score and Feedback			**TOTAL POINTS EARNED (20 max points)**	
☐ Exemplary	20	Outstanding understanding and application of VirtualBox OVA import and configuration.		
☐ Proficient	16-19	Good understanding with minor areas for improvement.		
☐ Developing	12-15	Basic understanding but requires significant improvement.		
☐ Beginning	8-11	Limited understanding with substantial need for improvement.		
☐ Not Attempted	0-7	Little to no understanding demonstrated.		

Evaluated by:	**Remarks/Comments**
_____ Name of Course Instructor	