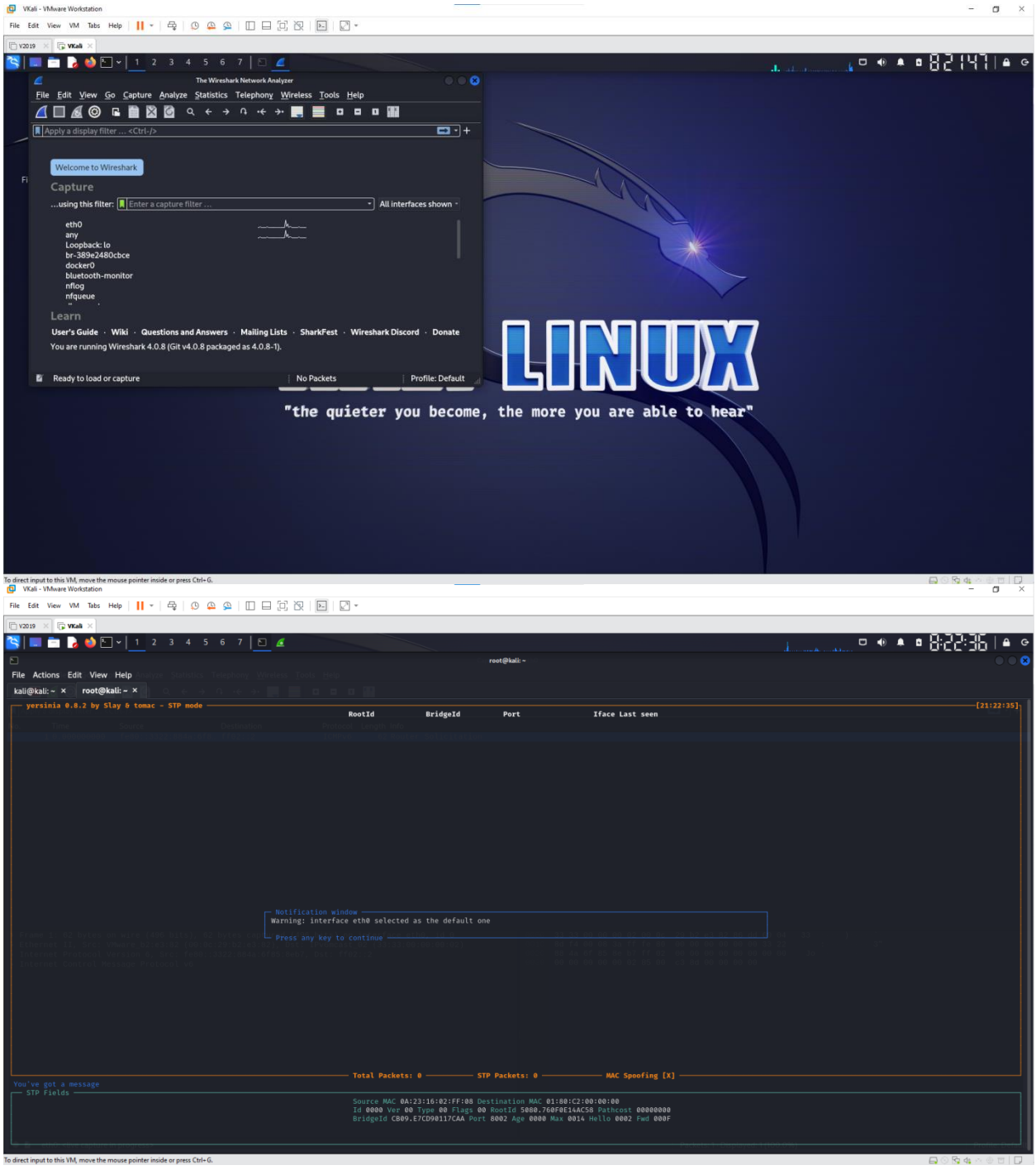
Lab 10: Sniffing

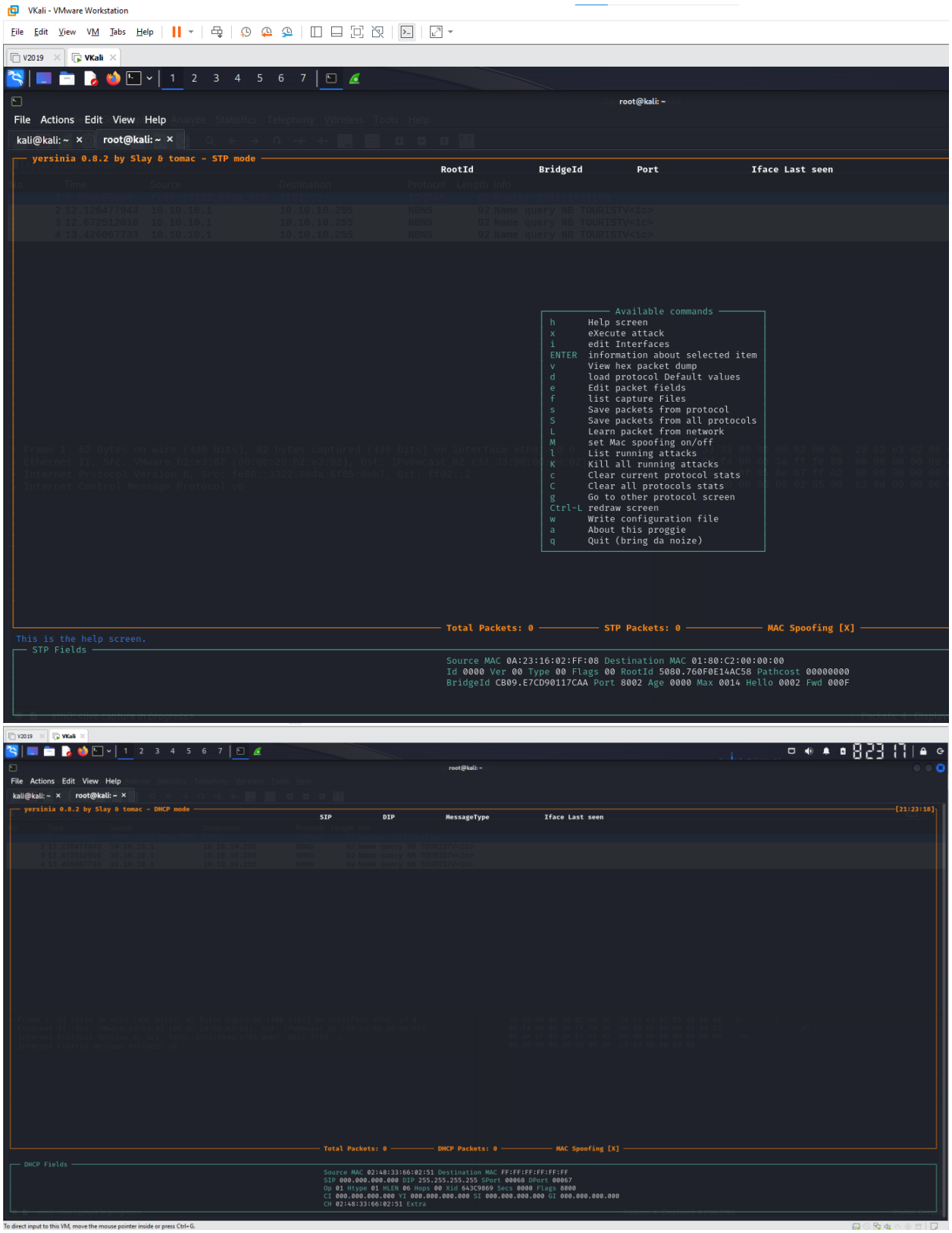
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 14/10/2023

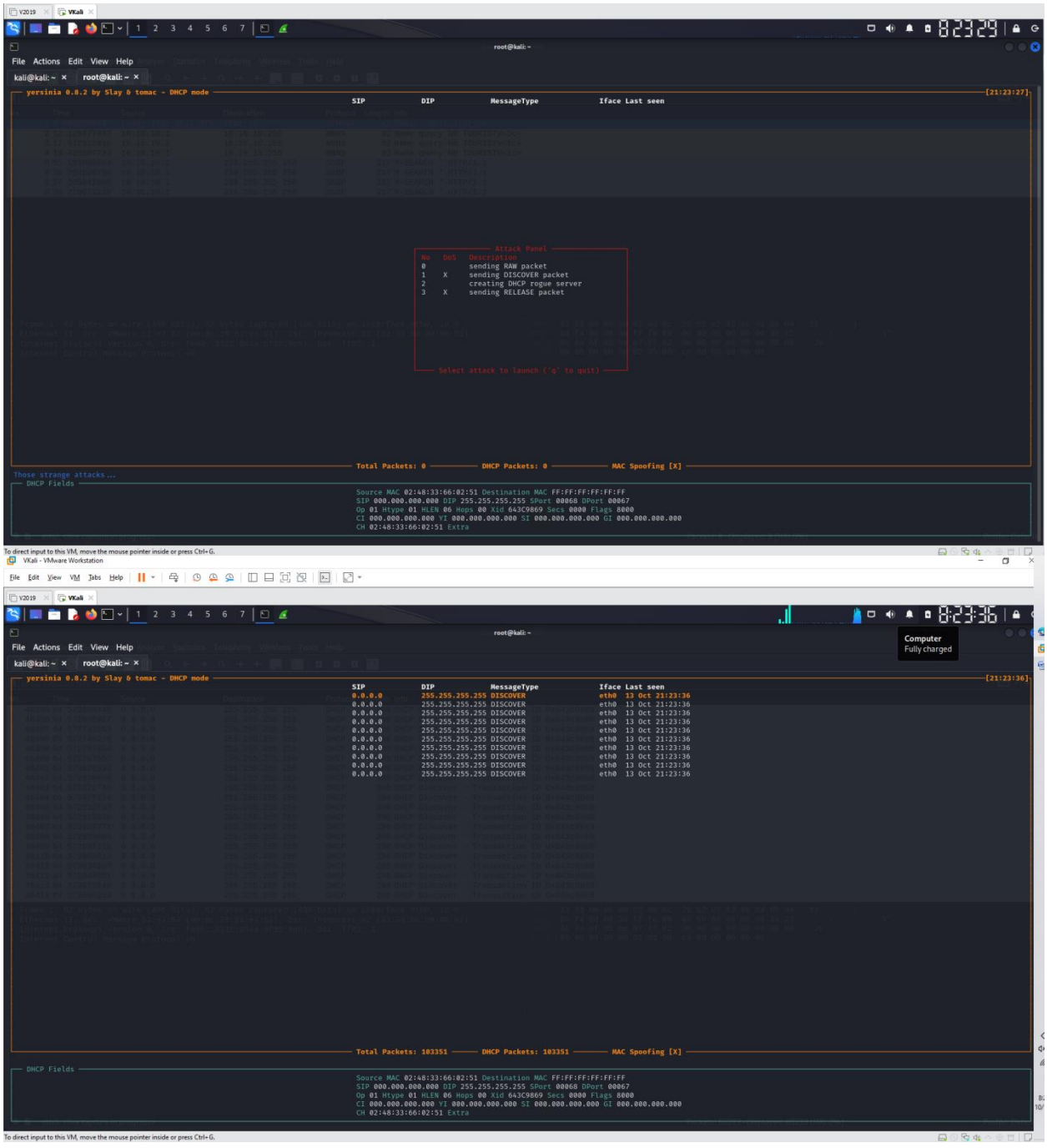
1. Perform Active Sniffing

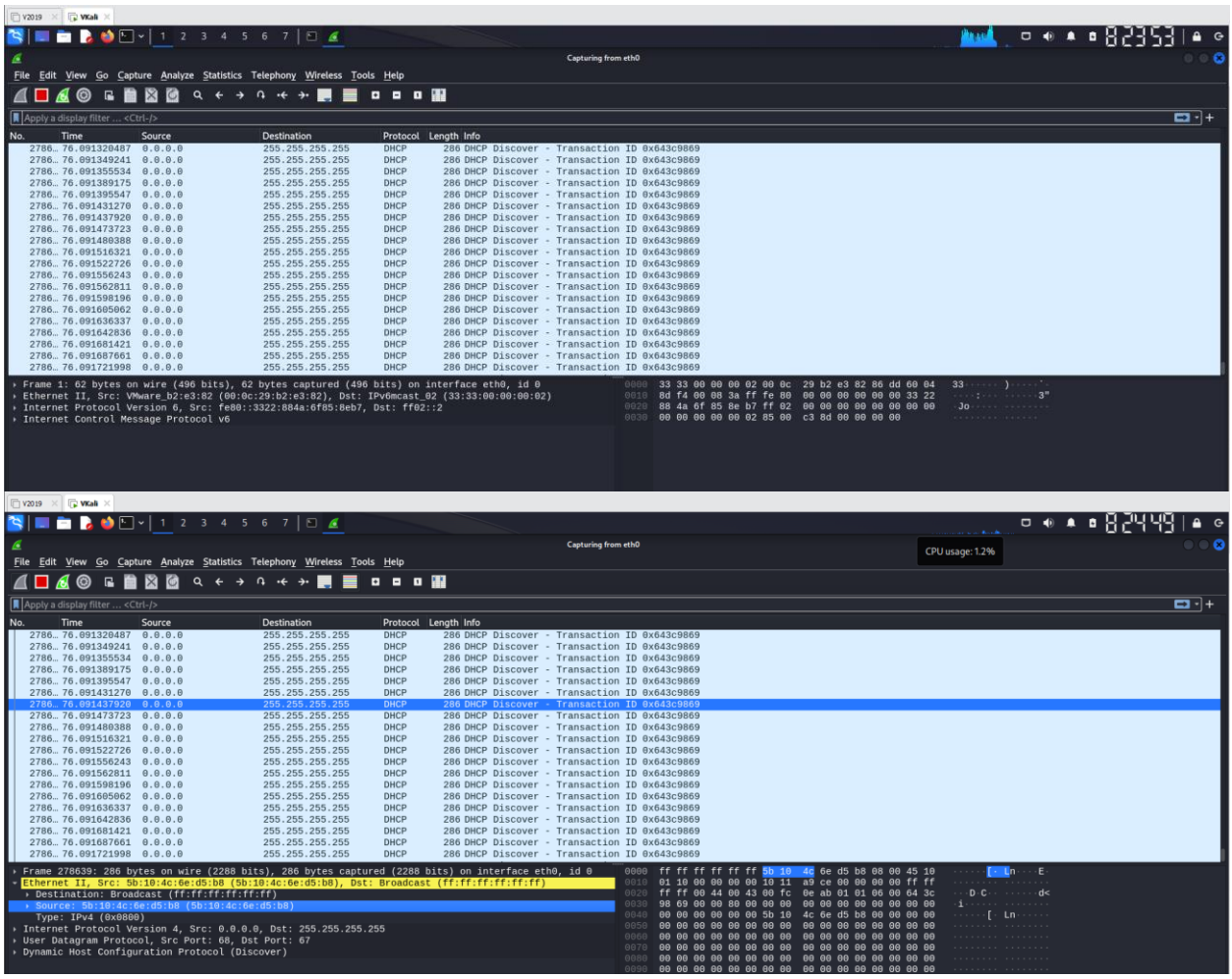
1.1 Perform a DHCP Starvation Attack using Yersinia

- Open Parrot


VKali - VMware Workstation
The Wireshark Network Analyzer
Welcome to Wireshark
Capture
Learn
LINUX
"the quieter you become, the more you are able to hear"
root@kali: ~
yersinia 0.8.2 by Slay & tomac - STP mode
Notification window
Warning: interface eth0 selected as the default one
Press any key to continue
Total Packets: 0
STP Packets: 0
MAC Spoofing [X]
STP Fields


VKali - VMware Workstation
File Edit View VM Tabs Help
V2019
VKali
File Actions Edit View Help
kali@kali: ~
root@kali: ~
yersinia 0.8.2 by Slay & tomac - STP mode
RootId
BridgeId
Port
Iface Last seen
Available commands
h Help screen
x eXecute attack
i edit Interfaces
ENTER information about selected item
v View hex packet dump
d load protocol Default values
e Edit packet fields
f list capture Files
s Save packets from protocol
S Save packets from all protocols
L Learn packet from network
M set Mac spoofing on/off
l List running attacks
K Kill all running attacks
c Clear current protocol stats
C Clear all protocols stats
g Go to other protocol screen
Ctrl-L redraw screen
w Write configuration file
a About this proggie
q Quit (bring da noize)
Total Packets: 0
STP Packets: 0
MAC Spoofing [X]
This is the help screen.
STP Fields
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
BridgeId CB09.E7CD90117CAA Port 8002 Age 0000 Max 0014 Hello 0002 Fwd 000F
yersinia 0.8.2 by Slay & tomac - DHCP mode
SIP
DIP
MessageType
Iface Last seen
Total Packets: 0
DHCP Packets: 0
MAC Spoofing [X]
DHCP Fields
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

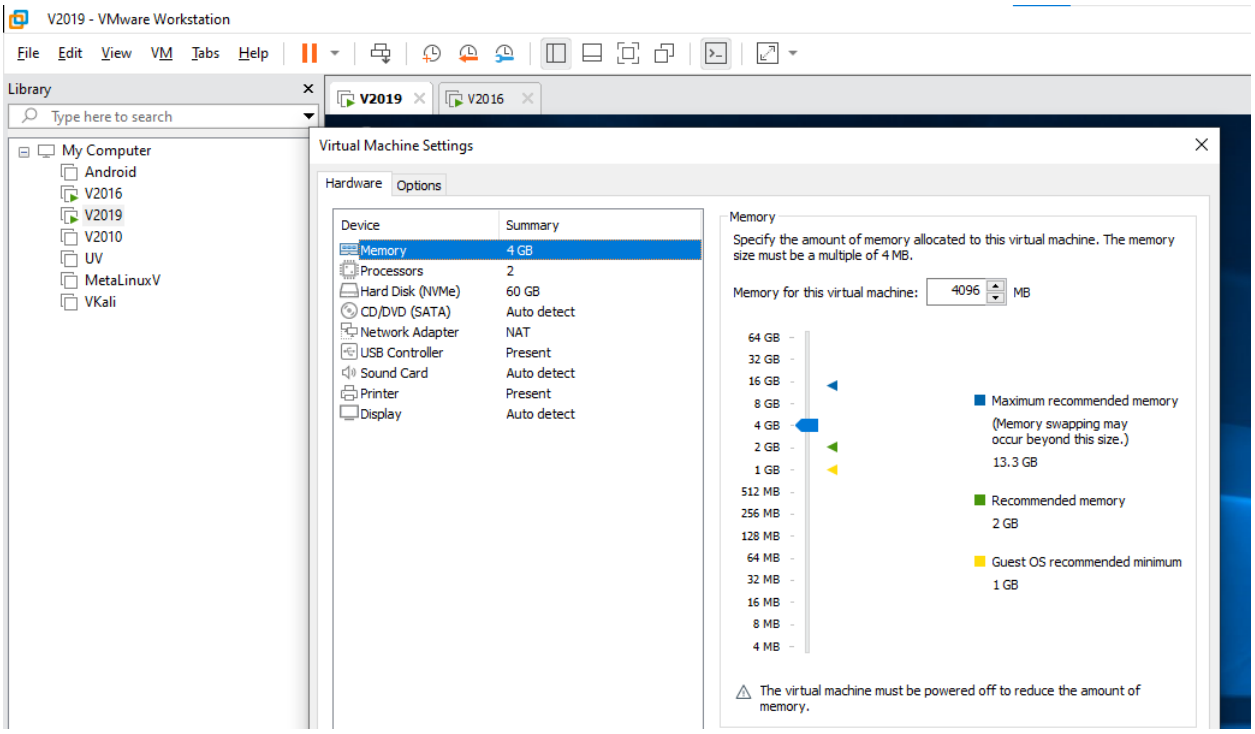

root@kali: ~
File Actions Edit View Help
kali@kali: ~
root@kali: ~
yersinia 0.8.2 by Slay & tomac - DHCP mode
SIP DIP MessageType Iface Last seen
[21:23:27]
Attack Panel
No DoS Description
0 sending RAW packet
1 X sending DISCOVER packet
2 creating DHCP rogue server
3 X sending RELEASE packet
Select attack to launch ('q' to quit)
Total Packets: 0
DHCP Packets: 0
MAC Spoofing [X]
Those strange attacks...
DHCP Fields
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
VKali - VMware Workstation
File Edit View VM Tabs Help
root@kali: ~
File Actions Edit View Help
kali@kali: ~
root@kali: ~
yersinia 0.8.2 by Slay & tomac - DHCP mode
SIP DIP MessageType Iface Last seen
[21:23:36]
0.0.0.0 255.255.255.255 DISCOVER eth0 13 Oct 21:23:36
0.0.0.0 255.255.255.255 DISCOVER eth0 13 Oct 21:23:36
Computer
Fully charged
Total Packets: 103351
DHCP Packets: 103351
MAC Spoofing [X]
DHCP Fields
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 YI 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CH 02:48:33:66:02:51 Extra
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

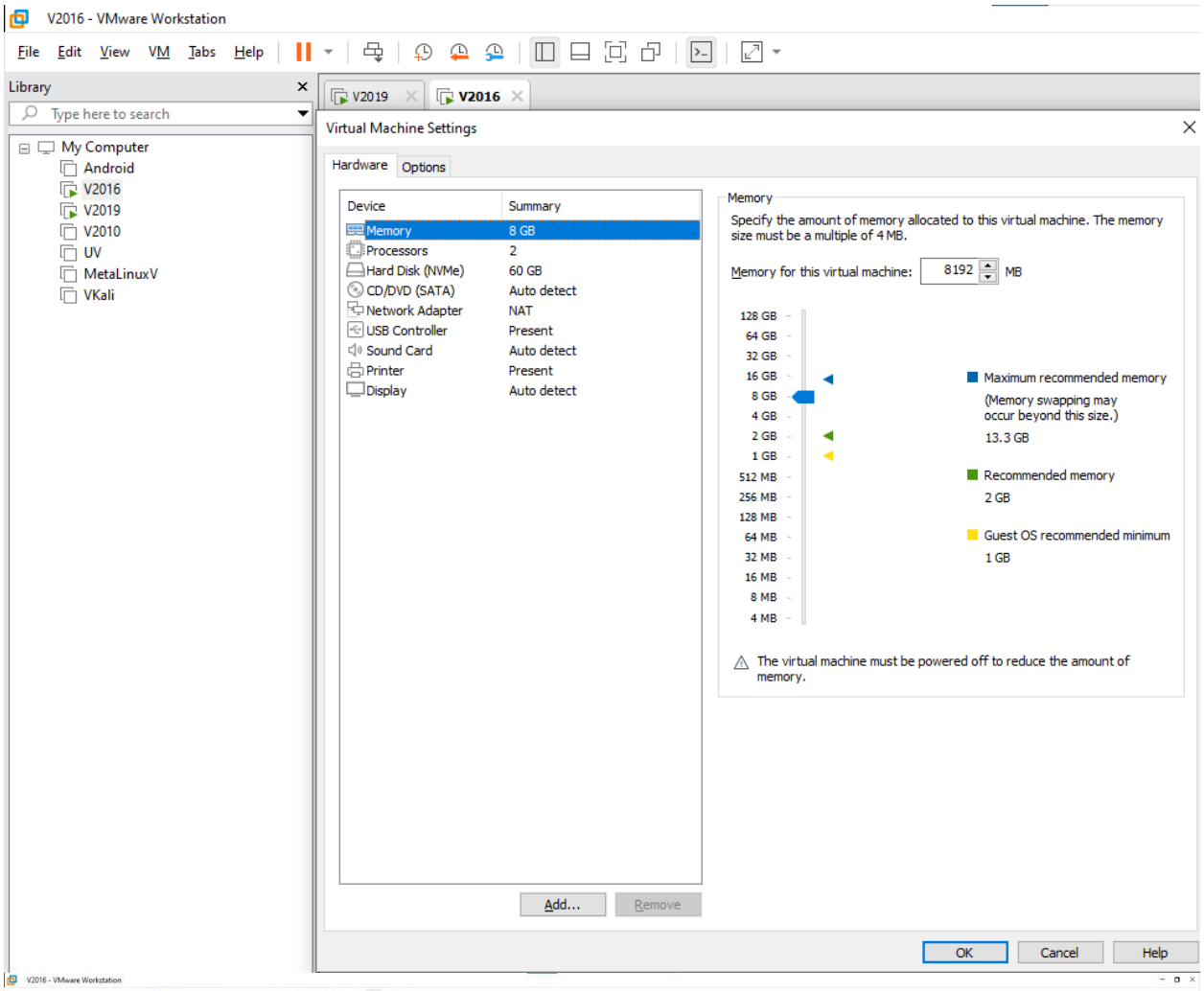


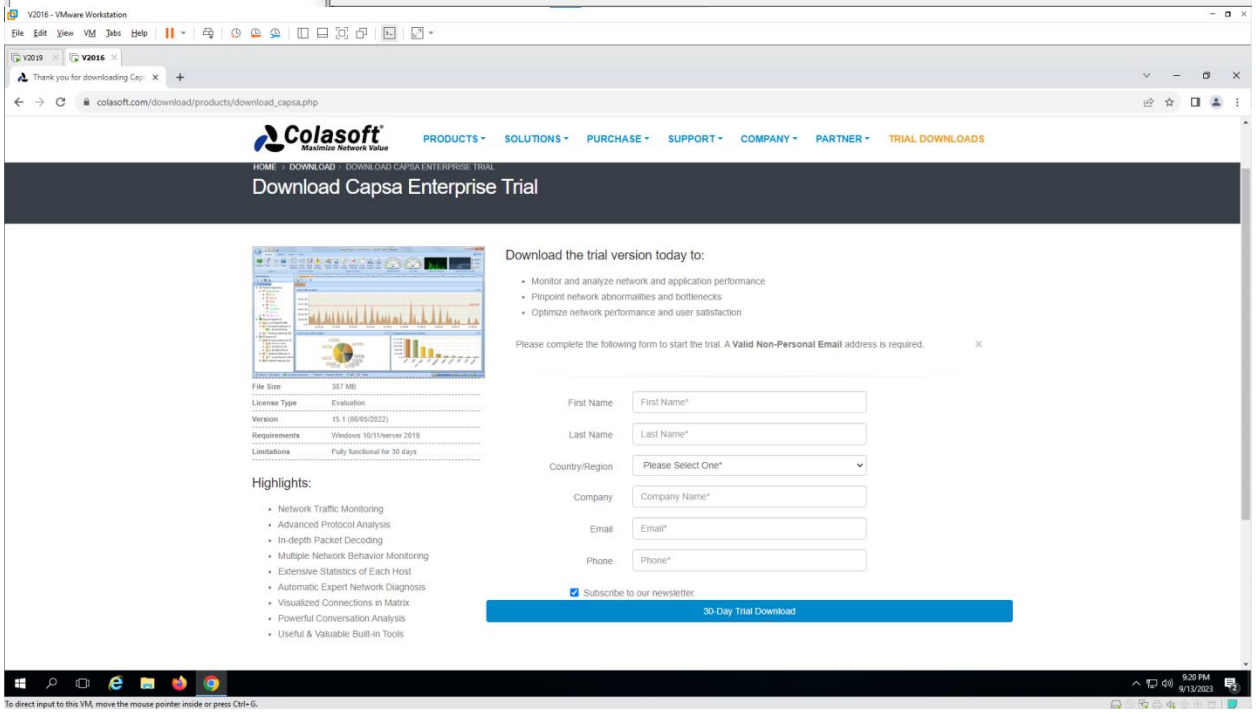
2. Perform Network Sniffing using Various Sniffing Tools

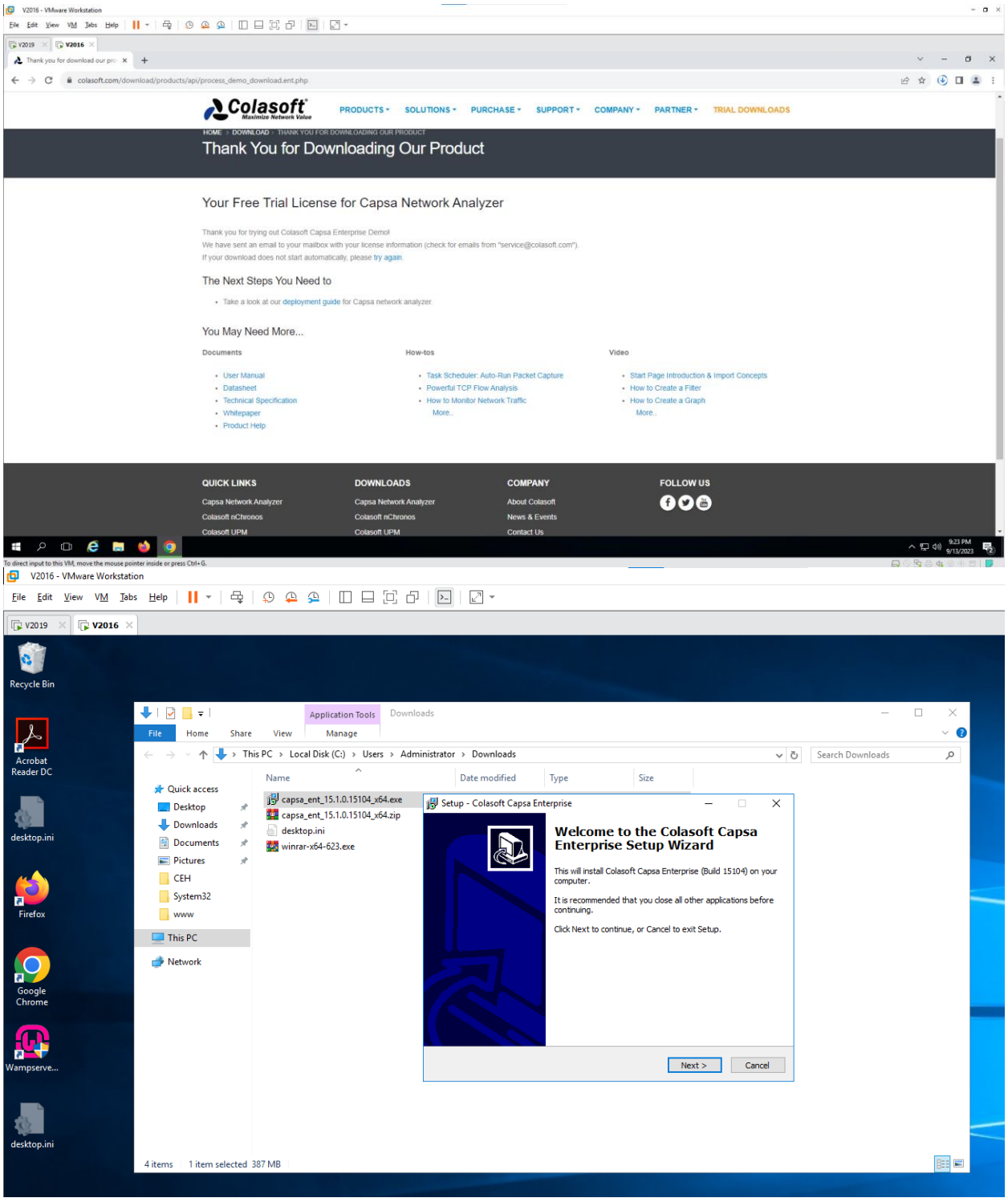
2.2 Analyze a Network using the Capsa Network Analyzer

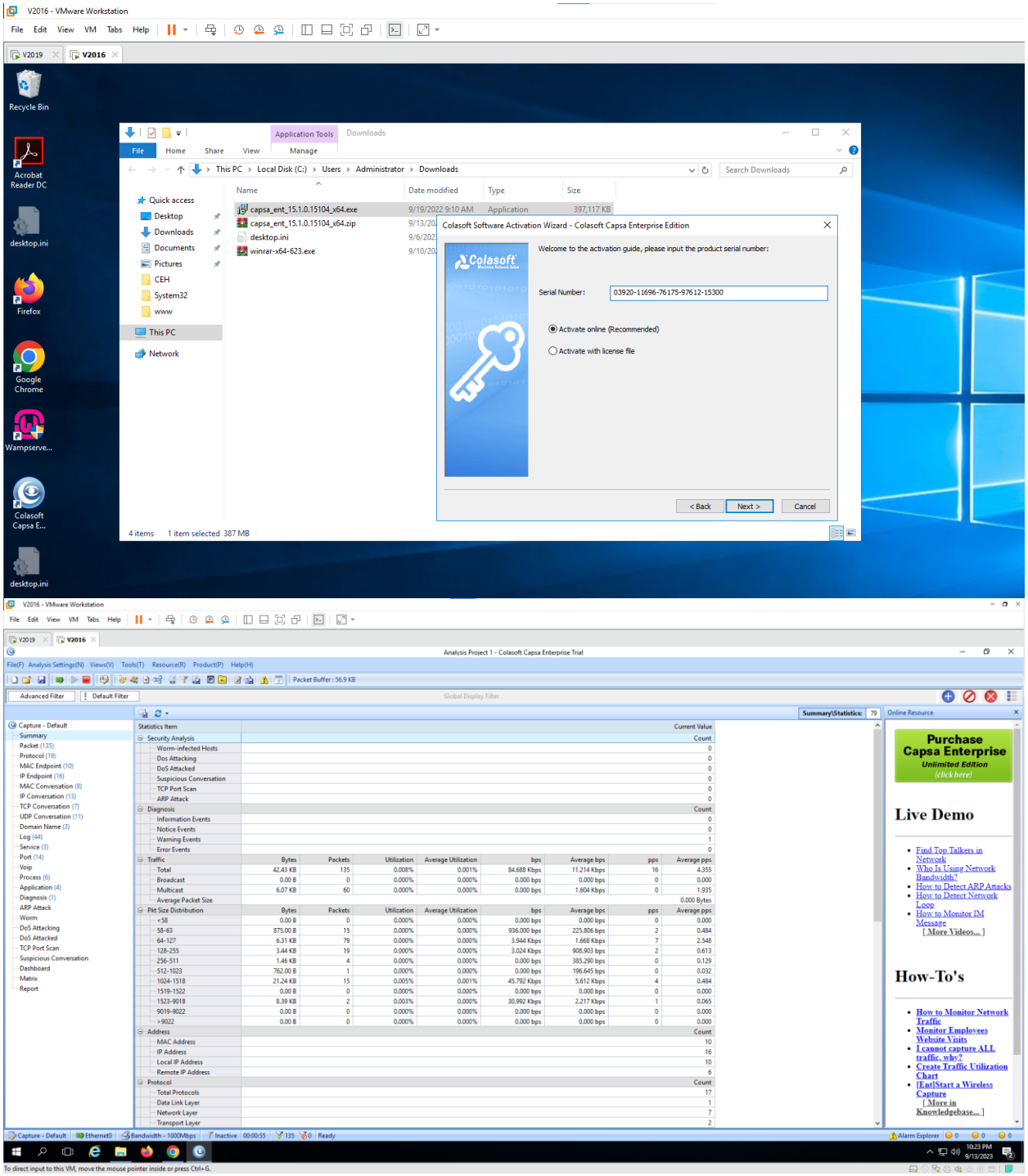
- Open Windows 10 and Windows Server 2019

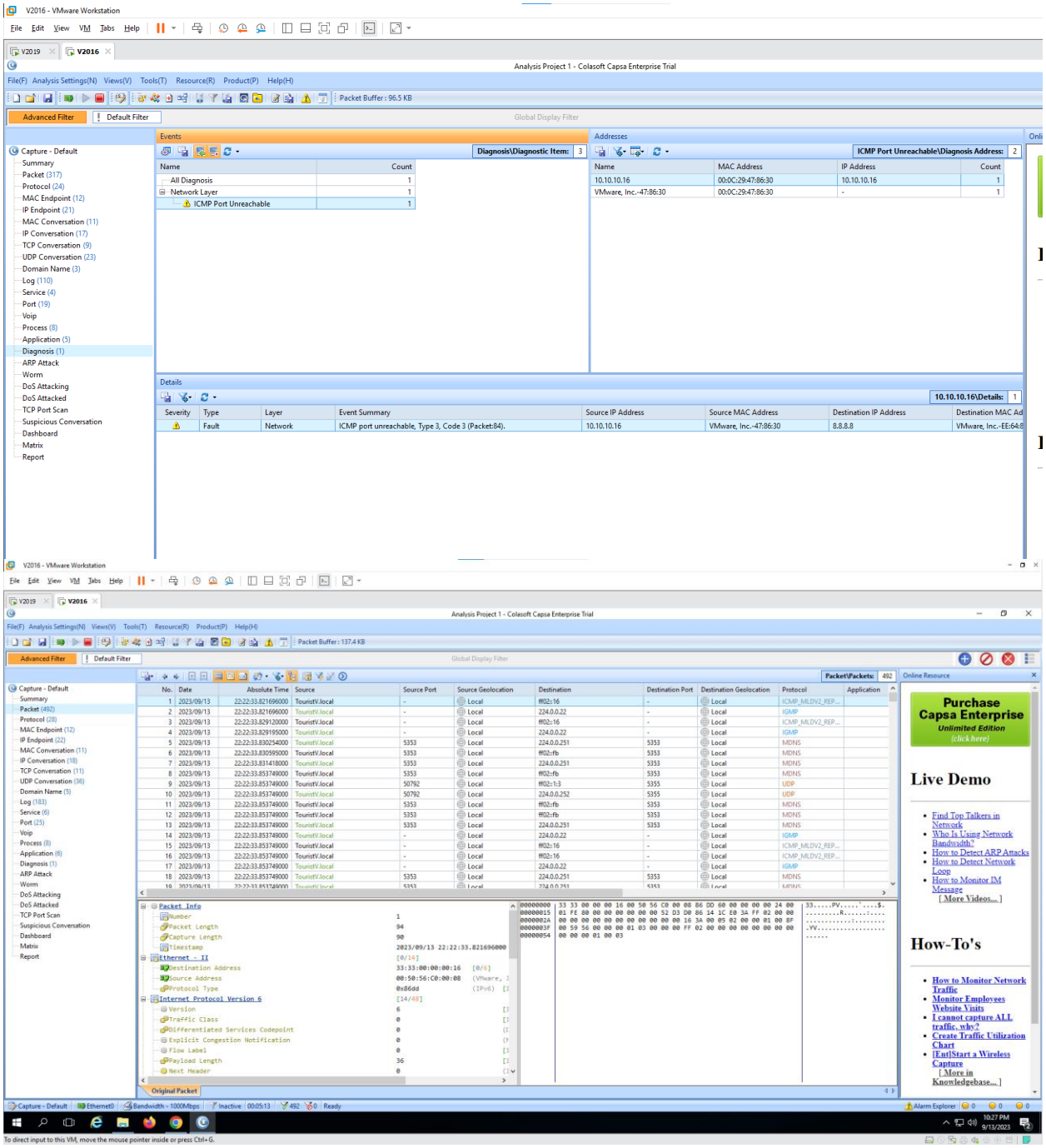

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
VKali
V2019
V2016
Virtual Machine Settings
Hardware
Options
Device
Summary
Memory 4 GB
Processors 2
Hard Disk (NVMe) 60 GB
CD/DVD (SATA) Auto detect
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine: 4096 MB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.3 GB
Recommended memory
2 GB
Guest OS recommended minimum
1 GB
The virtual machine must be powered off to reduce the amount of memory.

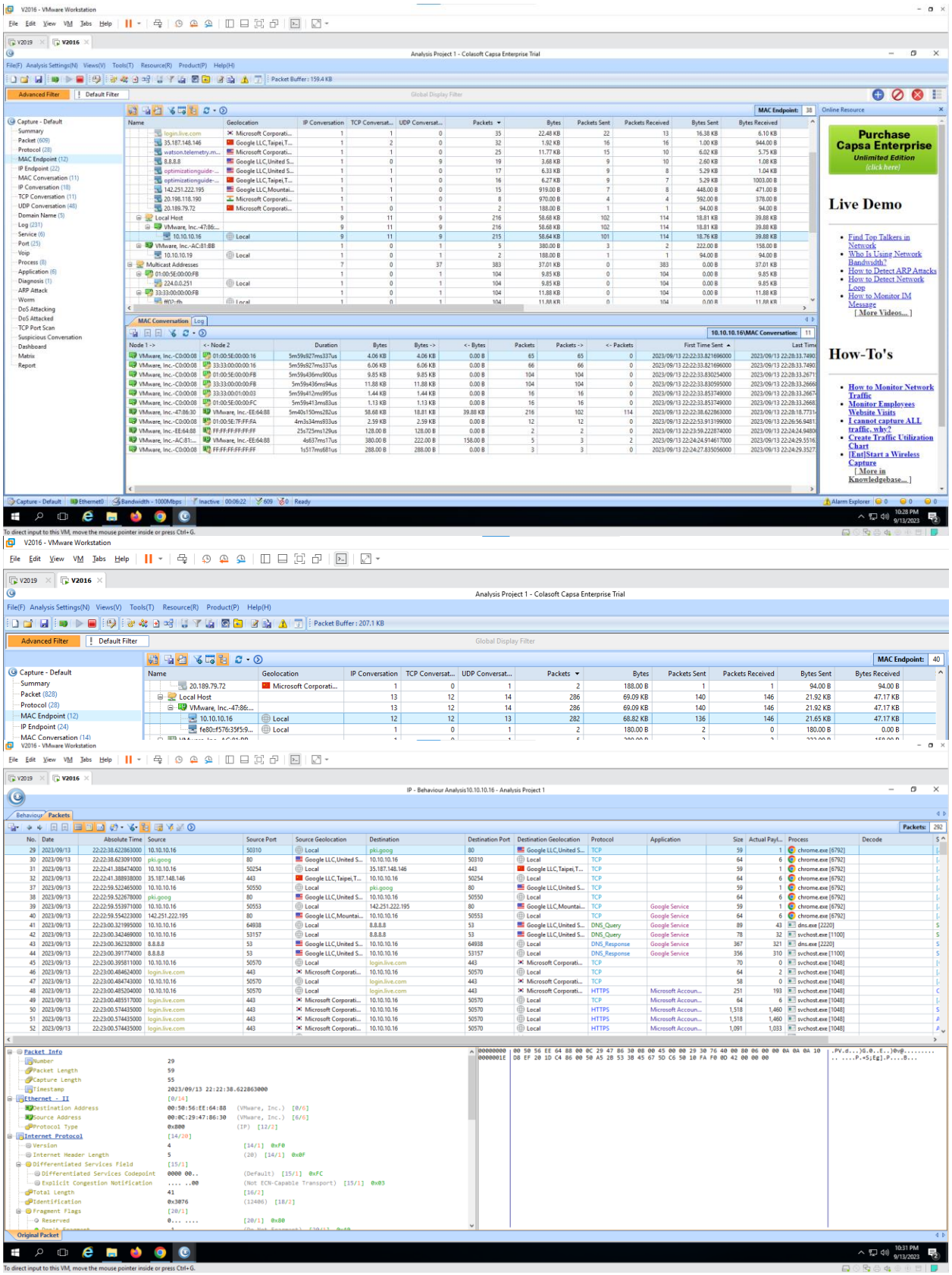

V2016 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
VKali
V2019
V2016
Virtual Machine Settings
Hardware
Options
Device
Summary
Memory 8 GB
Processors 2
Hard Disk (NVMe) 60 GB
CD/DVD (SATA) Auto detect
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Add...
Remove
Memory
Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.
Memory for this virtual machine: 8192 MB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.3 GB
Recommended memory
2 GB
Guest OS recommended minimum
1 GB
The virtual machine must be powered off to reduce the amount of memory.
OK
Cancel
Help

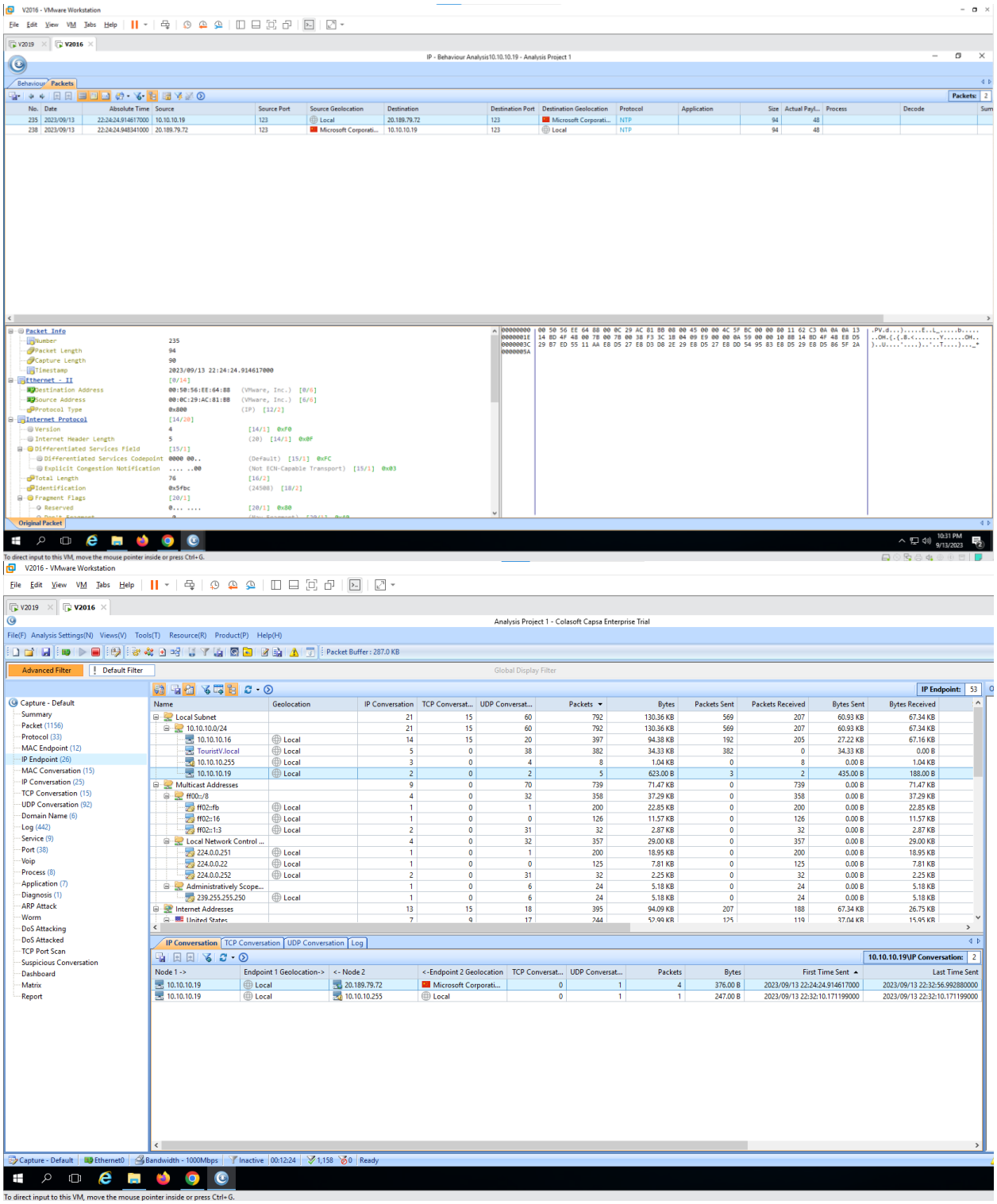

colasoft.com/download/products/download_capsa.php
Colasoft
Maximize Network Value
PRODUCTS
SOLUTIONS
PURCHASE
SUPPORT
COMPANY
PARTNER
TRIAL DOWNLOADS
HOME > DOWNLOAD > DOWNLOAD CAPSA ENTERPRISE TRIAL
Download Capsa Enterprise Trial
Download the trial version today to:
Monitor and analyze network and application performance
Pinpoint network abnormalities and bottlenecks
Optimize network performance and user satisfaction
Please complete the following form to start the trial. A Valid Non-Personal Email address is required.
First Name
Last Name
Country/Region
Please Select One*
Company
Email
Phone
Subscribe to our newsletter.
30-Day Trial Download
Highlights:
Network Traffic Monitoring
Advanced Protocol Analysis
In-depth Packet Decoding
Multiple Network Behavior Monitoring
Extensive Statistics of Each Host
Automatic Expert Network Diagnosis
Visualized Connections in Matrix
Powerful Conversation Analysis
Useful & Valuable Built-in Tools

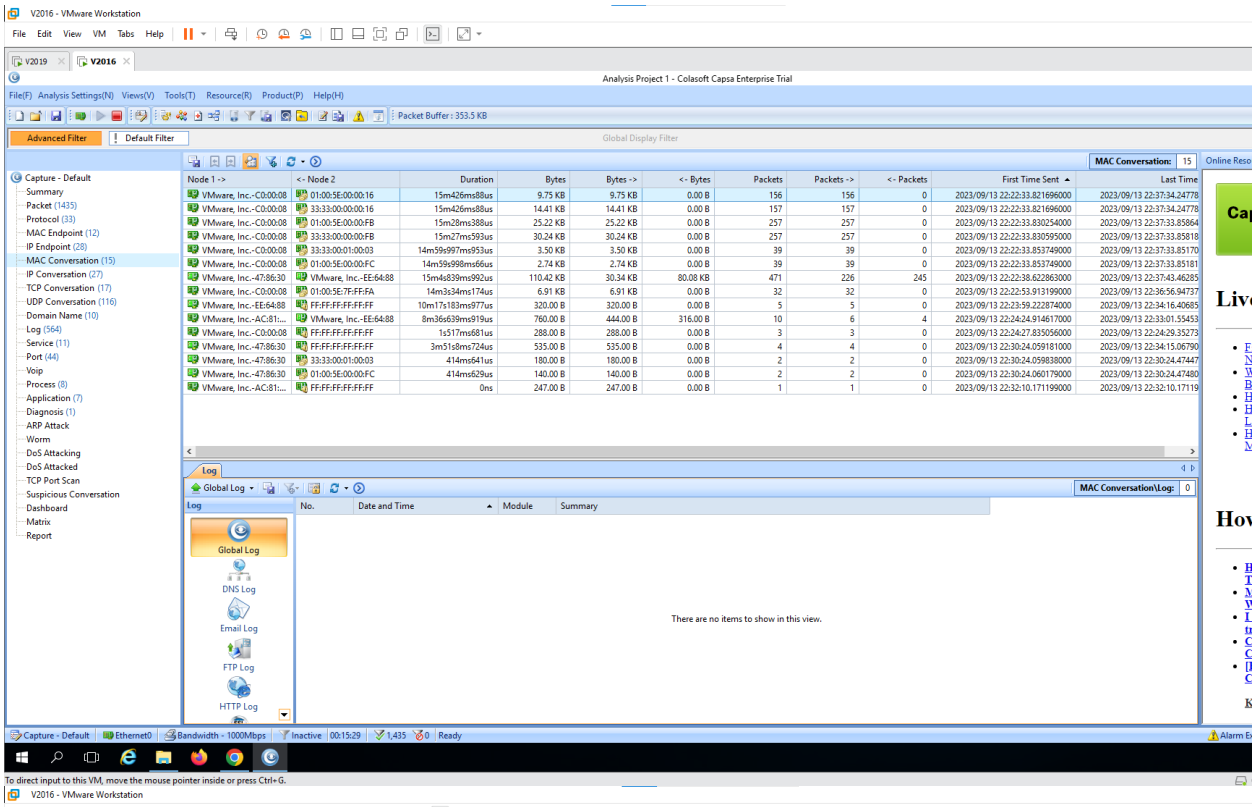

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
colasoft.com/download/products/api/process_demo_download.ent.php
Colasoft
Maximize Network Value
PRODUCTS
SOLUTIONS
PURCHASE
SUPPORT
COMPANY
PARTNER
TRIAL DOWNLOADS
HOME > DOWNLOAD > THANK YOU FOR DOWNLOADING OUR PRODUCT
Thank You for Downloading Our Product
Your Free Trial License for Capsa Network Analyzer
Thank you for trying out Colasoft Capsa Enterprise Demo!
We have sent an email to your mailbox with your license information (check for emails from "service@colasoft.com").
If your download does not start automatically, please try again.
The Next Steps You Need to
Take a look at our deployment guide for Capsa network analyzer.
You May Need More...
Documents
User Manual
Datasheet
Technical Specification
Whitepaper
Product Help
How-tos
Task Scheduler: Auto-Run Packet Capture
Powerful TCP Flow Analysis
How to Monitor Network Traffic
More..
Video
Start Page Introduction & Import Concepts
How to Create a Filter
How to Create a Graph
More..
QUICK LINKS
Capsa Network Analyzer
Colasoft nChronos
Colasoft UPM
DOWNLOADS
Capsa Network Analyzer
Colasoft nChronos
Colasoft UPM
COMPANY
About Colasoft
News & Events
Contact Us
FOLLOW US
9:23 PM
9/13/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
desktop.ini
Application Tools
Downloads
File
Home
Share
View
Manage
This PC > Local Disk (C:) > Users > Administrator > Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
capsa_ent_15.1.0.15104_x64.exe
capsa_ent_15.1.0.15104_x64.zip
desktop.ini
winrar-x64-623.exe
Setup - Colasoft Capsa Enterprise
Welcome to the Colasoft Capsa Enterprise Setup Wizard
This will install Colasoft Capsa Enterprise (Build 15104) on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel
4 items
1 item selected 387 MB

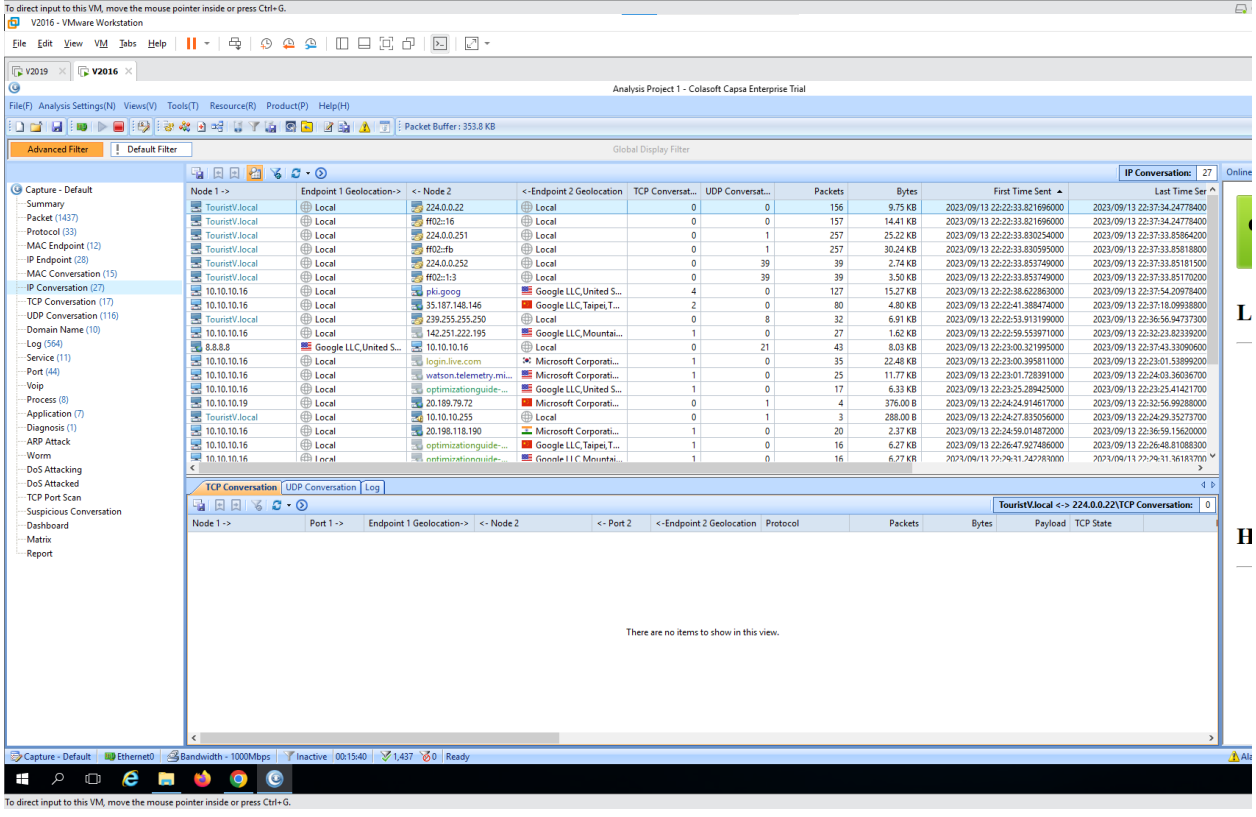

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Recycle Bin
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
Colasoft Capsa E...
desktop.ini
Application Tools
Downloads
File Home Share View Manage
This PC › Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
capsa_ent_15.1.0.15104_x64.exe 9/19/2022 9:10 AM Application 397,117 KB
capsa_ent_15.1.0.15104_x64.zip
desktop.ini
winrar-x64-623.exe
4 items 1 item selected 387 MB
Colasoft Software Activation Wizard - Colasoft Capsa Enterprise Edition
Welcome to the activation guide, please input the product serial number:
Serial Number:
03920-11696-76175-97612-15300
Activate online (Recommended)
Activate with license file
< Back
Next >
Cancel
Analysis Project 1 - Colasoft Capsa Enterprise Trial
Purchase Capsa Enterprise
Unlimited Edition
(click here)
Live Demo
Find Top Talkers in Network
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
[More Videos...]
How-To's
How to Monitor Network Traffic
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Esc]Start a Wireless Capture
[More in Knowledgebase...]

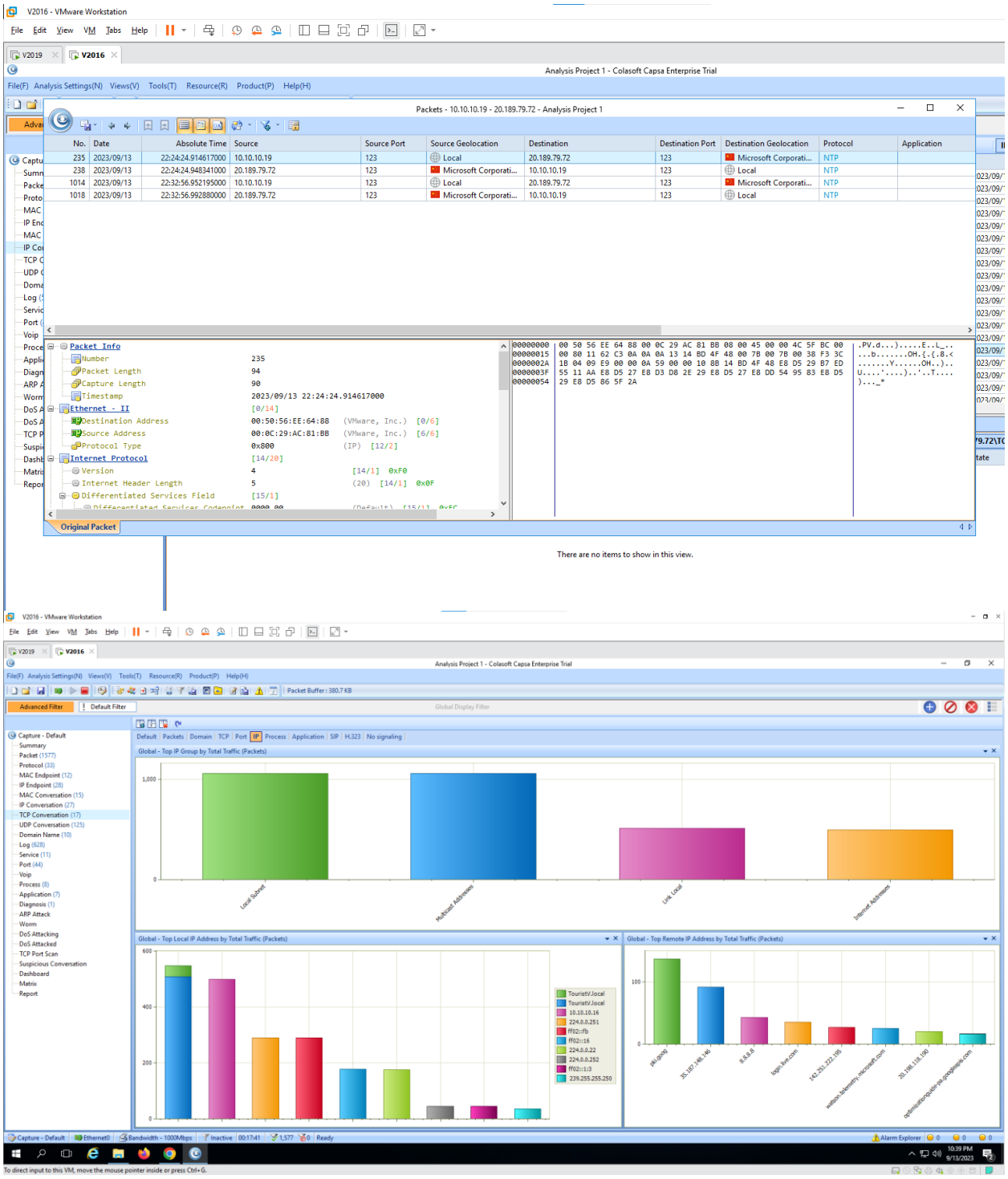

V2016 - VMware Workstation
Analysis Project 1 - Colasoft Capsa Enterprise Trial
Events
Addresses
Details
Capture - Default
Diagnosis
ICMP Port Unreachable
Purchase Capsa Enterprise
Unlimited Edition
Live Demo
How-To's

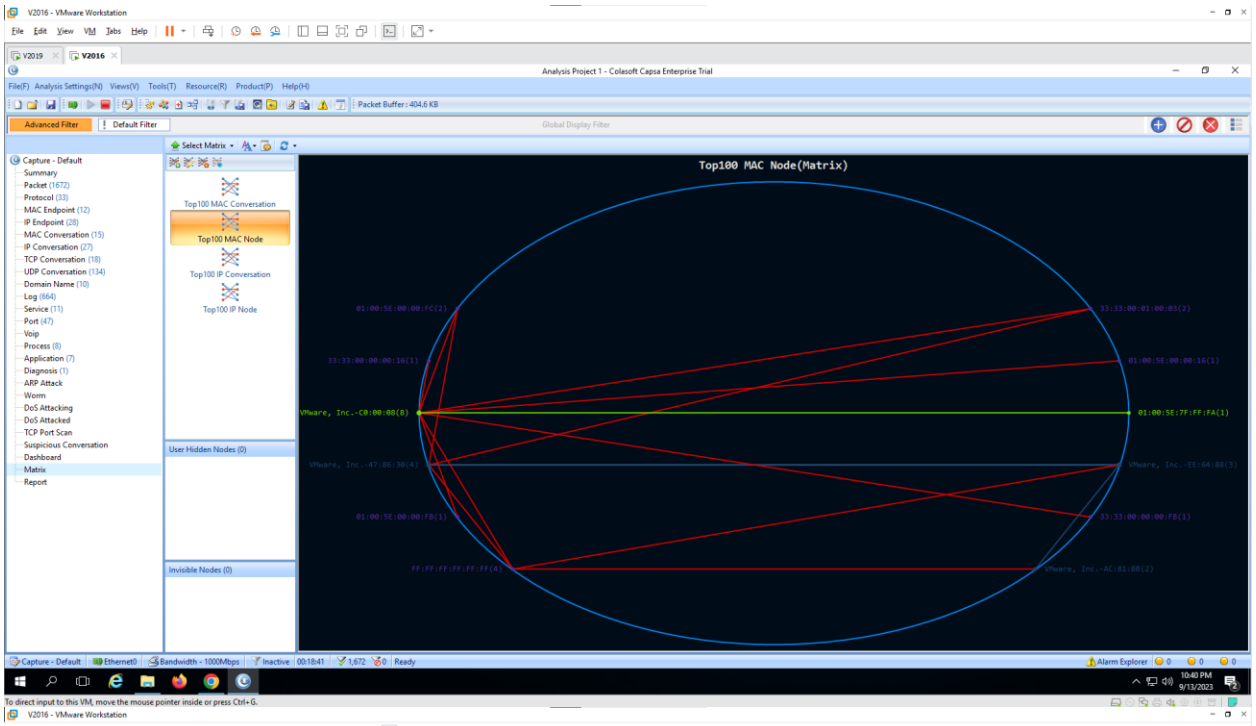

V2016 - VMware Workstation
Analysis Project 1 - Colasoft Capsa Enterprise Trial
Purchase Capsa Enterprise
Unlimited Edition
(click here)
Live Demo
Find Top Talkers in Network
Who Is Using Network Bandwidth?
How to Detect ARP Attacks
How to Detect Network Loop
How to Monitor IM Message
[More Videos...]
How-To's
How to Monitor Network Traffic
Monitor Employees Website Visits
I cannot capture ALL traffic, why?
Create Traffic Utilization Chart
[Ent]Start a Wireless Capture
[More in Knowledgebase...]
V2016 - VMware Workstation
Analysis Project 1 - Colasoft Capsa Enterprise Trial
V2016 - VMware Workstation
IP - Behaviour Analysis10.10.10.16 - Analysis Project 1

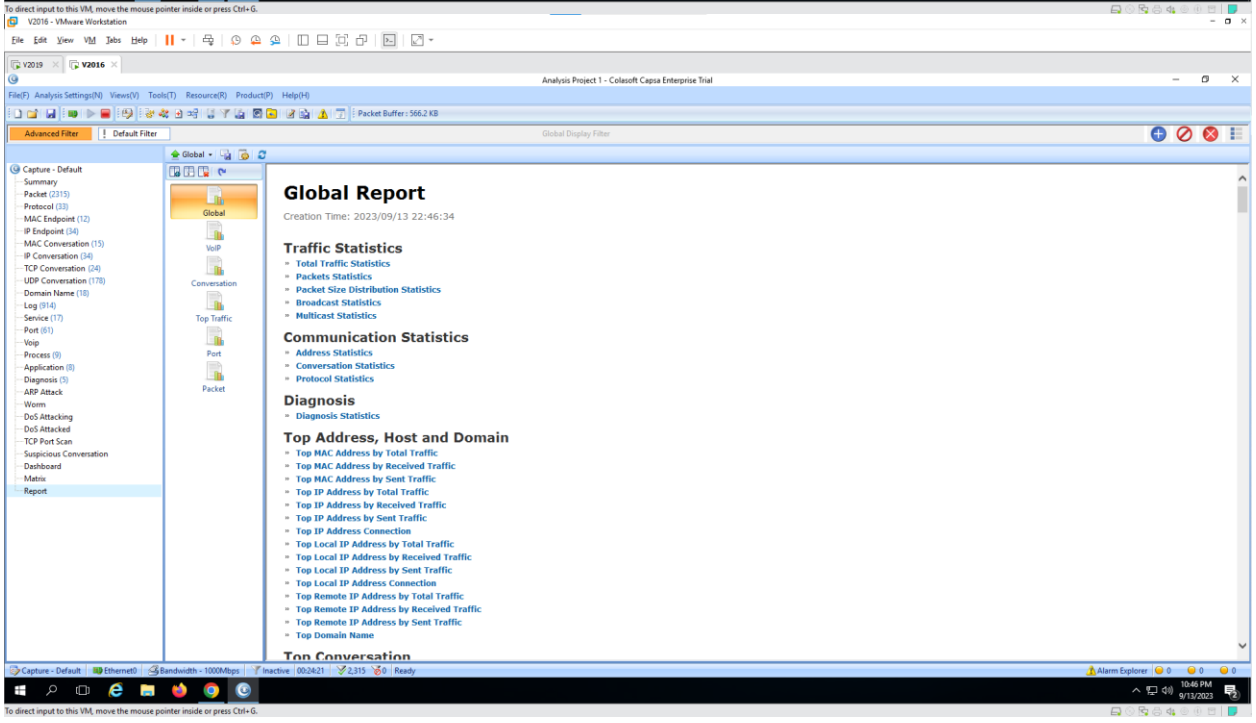

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
IP - Behaviour Analysis10.10.10.19 - Analysis Project 1
Behaviour
Packets
No. Date Absolute Time Source Source Port Source Geolocation Destination Destination Port Destination Geolocation Protocol Application Size Actual Payl... Process Decode
235 2023/09/13 22:24:24.914617000 10.10.10.19 123 Local 20.189.79.72 123 Microsoft Corporati... NTP 94 48
238 2023/09/13 22:24:24.948341000 20.189.79.72 123 Microsoft Corporati... 10.10.10.19 123 Local NTP 94 48
Packet Info
Number 235
Packet Length 94
Capture Length 90
Timestamp 2023/09/13 22:24:24.914617000
Ethernet - II [0/14]
Destination Address 00:50:56:EE:64:88 (VMware, Inc.) [0/6]
Source Address 00:0C:29:AC:81:88 (VMware, Inc.) [6/6]
Protocol Type 0x800 (IP) [12/2]
Internet Protocol [14/20]
Version 4 [14/1] 0xF0
Internet Header Length 5 (20) [14/1] 0x0F
Differentiated Services Field [15/1]
Differentiated Services Codepoint 0000 00.. (Default) [15/1] 0xFC
Explicit Congestion Notification .... ..00 (Not ECN-Capable Transport) [15/1] 0x03
Total Length 76 [16/2]
Identification 0x5fbc (24508) [18/2]
Fragment Flags [20/1]
Reserved 0... .... [20/1] 0x80
Original Packet
00000000 00 50 56 EE 64 88 00 0C 29 AC 81 88 08 00 45 00 00 4C 5F BC 00 00 80 11 62 C3 0A 0A 0A 13
0000001E 14 BD 4F 48 00 7B 00 7B 00 38 F3 3C 18 04 09 E9 00 00 0A 59 00 00 10 88 14 BD 4F 48 E8 D5
0000003C 29 B7 ED 55 11 AA E8 D5 27 E8 D3 D8 2E 29 E8 D5 27 E8 DD 54 95 83 E8 D5 29 E8 D5 86 5F 2A
0000005A
10:31 PM
9/13/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Analysis Project 1 - Colasoft Capsa Enterprise Trial
File(F) Analysis Settings(N) Views(V) Tools(T) Resource(R) Product(P) Help(H)
Packet Buffer : 287.0 KB
Advanced Filter
Default Filter
Global Display Filter
IP Endpoint: 53
Capture - Default
Summary
Packet (1156)
Protocol (33)
MAC Endpoint (12)
IP Endpoint (26)
MAC Conversation (15)
IP Conversation (25)
TCP Conversation (15)
UDP Conversation (92)
Domain Name (6)
Log (442)
Service (9)
Port (38)
Voip
Process (8)
Application (7)
Diagnosis (1)
ARP Attack
Worm
DoS Attacking
DoS Attacked
TCP Port Scan
Suspicious Conversation
Dashboard
Matrix
Report
Name Geolocation IP Conversation TCP Conversat... UDP Conversat... Packets Bytes Packets Sent Packets Received Bytes Sent Bytes Received
Local Subnet 21 15 60 792 130.36 KB 569 207 60.93 KB 67.34 KB
10.10.10.0/24 21 15 60 792 130.36 KB 569 207 60.93 KB 67.34 KB
10.10.10.16 Local 14 15 20 397 94.38 KB 192 205 27.22 KB 67.16 KB
TouristV.local Local 5 0 38 382 34.33 KB 382 0 34.33 KB 0.00 B
10.10.10.255 Local 3 0 4 8 1.04 KB 0 8 0.00 B 1.04 KB
10.10.10.19 Local 2 0 2 5 623.00 B 3 2 435.00 B 188.00 B
Multicast Addresses 9 0 70 739 71.47 KB 0 739 0.00 B 71.47 KB
ff00::/8 4 0 32 358 37.29 KB 0 358 0.00 B 37.29 KB
ff02::fb Local 1 0 1 200 22.85 KB 0 200 0.00 B 22.85 KB
ff02::16 Local 1 0 0 126 11.57 KB 0 126 0.00 B 11.57 KB
ff02::1:3 Local 2 0 31 32 2.87 KB 0 32 0.00 B 2.87 KB
Local Network Control ... 4 0 32 357 29.00 KB 0 357 0.00 B 29.00 KB
224.0.0.251 Local 1 0 1 200 18.95 KB 0 200 0.00 B 18.95 KB
224.0.0.22 Local 1 0 0 125 7.81 KB 0 125 0.00 B 7.81 KB
224.0.0.252 Local 2 0 31 32 2.25 KB 0 32 0.00 B 2.25 KB
Administratively Scope... 1 0 6 24 5.18 KB 0 24 0.00 B 5.18 KB
239.255.255.250 Local 1 0 6 24 5.18 KB 0 24 0.00 B 5.18 KB
Internet Addresses 13 15 18 395 94.09 KB 207 188 67.34 KB 26.75 KB
United States 7 9 17 244 52.99 KB 125 119 37.04 KB 15.95 KB
IP Conversation TCP Conversation UDP Conversation Log
10.10.10.19\IP Conversation: 2
Node 1 -> Endpoint 1 Geolocation-> <- Node 2 <-Endpoint 2 Geolocation TCP Conversat... UDP Conversat... Packets Bytes First Time Sent Last Time Sent
10.10.10.19 Local 20.189.79.72 Microsoft Corporati... 0 1 4 376.00 B 2023/09/13 22:24:24.914617000 2023/09/13 22:32:56.992880000
10.10.10.19 Local 10.10.10.255 Local 0 1 1 247.00 B 2023/09/13 22:32:10.171199000 2023/09/13 22:32:10.171199000
Capture - Default
Ethernet0
Bandwidth - 1000Mbps
Inactive
00:12:24
1,158
0
Ready
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

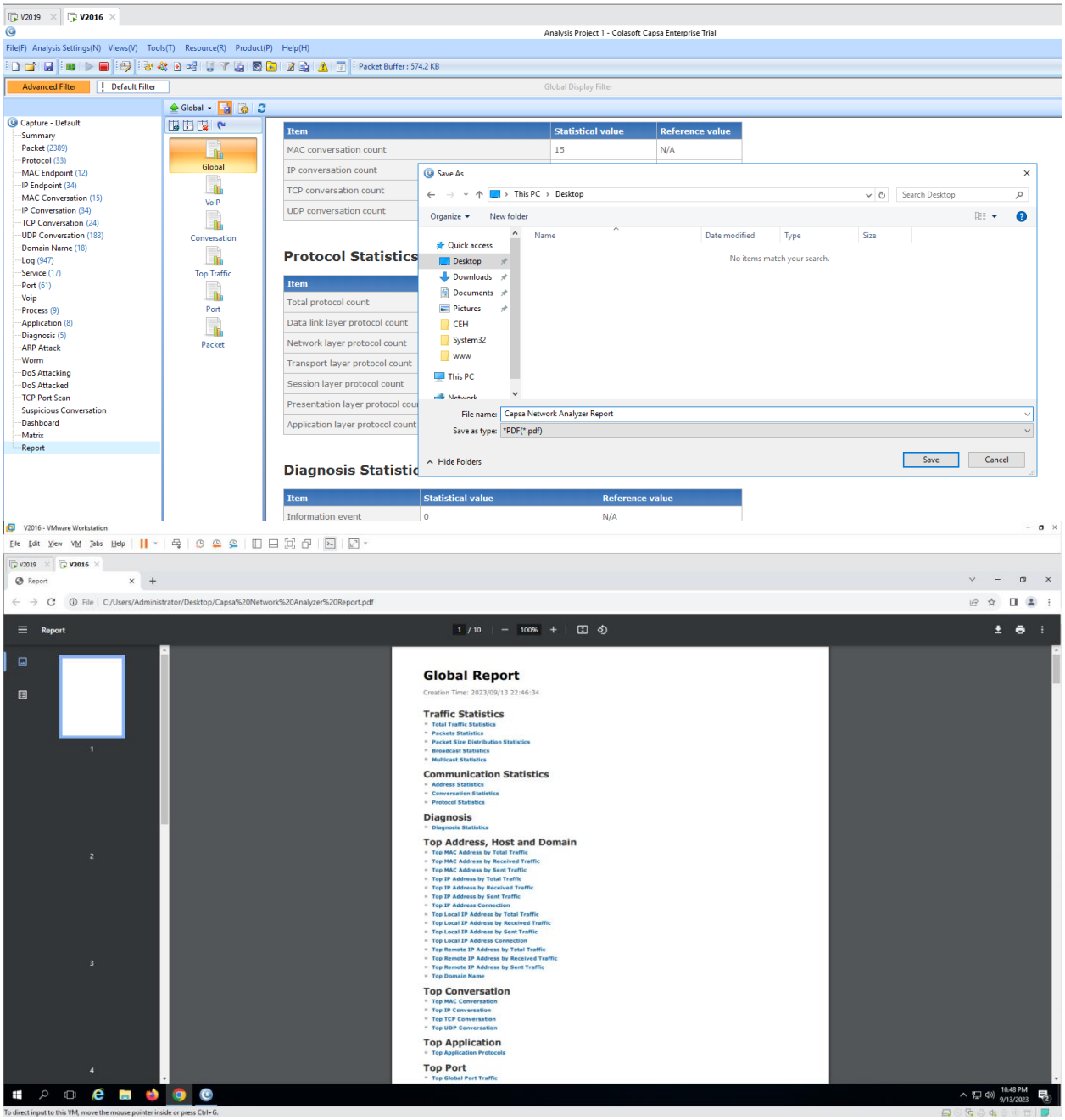

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Analysis Project 1 - Colasoft Capsa Enterprise Trial
File(F) Analysis Settings(N) Views(V) Tools(T) Resource(R) Product(P) Help(H)
Packet Buffer : 353.5 KB
Advanced Filter
Default Filter
Global Display Filter
MAC Conversation: 15
Capture - Default
Summary
Packet (1435)
Protocol (33)
MAC Endpoint (12)
IP Endpoint (28)
MAC Conversation (15)
IP Conversation (27)
TCP Conversation (17)
UDP Conversation (116)
Domain Name (10)
Log (564)
Service (11)
Port (44)
Voip
Process (8)
Application (7)
Diagnosis (1)
ARP Attack
Worm
DoS Attacking
DoS Attacked
TCP Port Scan
Suspicious Conversation
Dashboard
Matrix
Report
Node 1 -> | <- Node 2 | Duration | Bytes | Bytes -> | <- Bytes | Packets | Packets -> | <- Packets | First Time Sent | Last Time
VMware, Inc.-C0:00:08 | 01:00:5E:00:00:16 | 15m426ms88us | 9.75 KB | 9.75 KB | 0.00 B | 156 | 156 | 0 | 2023/09/13 22:22:33.821696000 | 2023/09/13 22:37:34.24778
VMware, Inc.-C0:00:08 | 33:33:00:00:00:16 | 15m426ms88us | 14.41 KB | 14.41 KB | 0.00 B | 157 | 157 | 0 | 2023/09/13 22:22:33.821696000 | 2023/09/13 22:37:34.24778
VMware, Inc.-C0:00:08 | 01:00:5E:00:00:FB | 15m28ms388us | 25.22 KB | 25.22 KB | 0.00 B | 257 | 257 | 0 | 2023/09/13 22:22:33.830254000 | 2023/09/13 22:37:33.85864
VMware, Inc.-C0:00:08 | 33:33:00:00:00:FB | 15m27ms593us | 30.24 KB | 30.24 KB | 0.00 B | 257 | 257 | 0 | 2023/09/13 22:22:33.830595000 | 2023/09/13 22:37:33.85818
VMware, Inc.-C0:00:08 | 33:33:00:01:00:03 | 14m59s997ms953us | 3.50 KB | 3.50 KB | 0.00 B | 39 | 39 | 0 | 2023/09/13 22:22:33.853749000 | 2023/09/13 22:37:33.85170
VMware, Inc.-C0:00:08 | 01:00:5E:00:00:FC | 14m59s998ms66us | 2.74 KB | 2.74 KB | 0.00 B | 39 | 39 | 0 | 2023/09/13 22:22:33.853749000 | 2023/09/13 22:37:33.85181
VMware, Inc.-47:86:30 | VMware, Inc.-EE:64:88 | 15m4s839ms992us | 110.42 KB | 30.34 KB | 80.08 KB | 471 | 226 | 245 | 2023/09/13 22:22:38.622863000 | 2023/09/13 22:37:43.46285
VMware, Inc.-C0:00:08 | 01:00:5E:7F:FF:FA | 14m3s34ms174us | 6.91 KB | 6.91 KB | 0.00 B | 32 | 32 | 0 | 2023/09/13 22:22:53.913199000 | 2023/09/13 22:36:56.94737
VMware, Inc.-EE:64:88 | FF:FF:FF:FF:FF:FF | 10m17s183ms977us | 320.00 B | 320.00 B | 0.00 B | 5 | 5 | 0 | 2023/09/13 22:23:59.222874000 | 2023/09/13 22:34:16.40685
VMware, Inc.-AC:81:... | VMware, Inc.-EE:64:88 | 8m36s639ms919us | 760.00 B | 444.00 B | 316.00 B | 10 | 6 | 4 | 2023/09/13 22:24:24.914617000 | 2023/09/13 22:33:01.55453
VMware, Inc.-C0:00:08 | FF:FF:FF:FF:FF:FF | 1s517ms681us | 288.00 B | 288.00 B | 0.00 B | 3 | 3 | 0 | 2023/09/13 22:24:27.835056000 | 2023/09/13 22:24:29.35273
VMware, Inc.-47:86:30 | FF:FF:FF:FF:FF:FF | 3m51s8ms724us | 535.00 B | 535.00 B | 0.00 B | 4 | 4 | 0 | 2023/09/13 22:30:24.059181000 | 2023/09/13 22:34:15.06790
VMware, Inc.-47:86:30 | 33:33:00:01:00:03 | 414ms641us | 180.00 B | 180.00 B | 0.00 B | 2 | 2 | 0 | 2023/09/13 22:30:24.209838000 | 2023/09/13 22:30:24.47447
VMware, Inc.-47:86:30 | 01:00:5E:00:00:FC | 414ms629us | 140.00 B | 140.00 B | 0.00 B | 2 | 2 | 0 | 2023/09/13 22:30:24.060179000 | 2023/09/13 22:30:24.47480
VMware, Inc.-AC:81:... | FF:FF:FF:FF:FF:FF | 0ns | 247.00 B | 247.00 B | 0.00 B | 1 | 1 | 0 | 2023/09/13 22:32:10.171199000 | 2023/09/13 22:32:10.17119
Log
Global Log
MAC Conversation\Log: 0
Log
No. | Date and Time | Module | Summary
Global Log
DNS Log
Email Log
FTP Log
HTTP Log
There are no items to show in this view.
Capture - Default | Ethernet0 | Bandwidth - 1000Mbps | Inactive | 00:15:29 | 1,435 | 0 | Ready
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Analysis Project 1 - Colasoft Capsa Enterprise Trial
File(F) Analysis Settings(N) Views(V) Tools(T) Resource(R) Product(P) Help(H)
Packet Buffer : 353.8 KB
Advanced Filter
Default Filter
Global Display Filter
IP Conversation: 27
Capture - Default
Summary
Packet (1437)
Protocol (33)
MAC Endpoint (12)
IP Endpoint (28)
MAC Conversation (15)
IP Conversation (27)
TCP Conversation (17)
UDP Conversation (116)
Domain Name (10)
Log (564)
Service (11)
Port (44)
Voip
Process (8)
Application (7)
Diagnosis (1)
ARP Attack
Worm
DoS Attacking
DoS Attacked
TCP Port Scan
Suspicious Conversation
Dashboard
Matrix
Report
Node 1 -> | Endpoint 1 Geolocation-> | <- Node 2 | <-Endpoint 2 Geolocation | TCP Conversat... | UDP Conversat... | Packets | Bytes | First Time Sent | Last Time Ser
TouristV.local | Local | 224.0.0.22 | Local | 0 | 0 | 156 | 9.75 KB | 2023/09/13 22:22:33.821696000 | 2023/09/13 22:37:34.24778400
TouristV.local | Local | ff02::16 | Local | 0 | 0 | 157 | 14.41 KB | 2023/09/13 22:22:33.821696000 | 2023/09/13 22:37:34.24778400
TouristV.local | Local | 224.0.0.251 | Local | 0 | 1 | 257 | 25.22 KB | 2023/09/13 22:22:33.830254000 | 2023/09/13 22:37:33.85864200
TouristV.local | Local | ff02::fb | Local | 0 | 1 | 257 | 30.24 KB | 2023/09/13 22:22:33.830595000 | 2023/09/13 22:37:33.85818800
TouristV.local | Local | 224.0.0.252 | Local | 0 | 39 | 39 | 2.74 KB | 2023/09/13 22:22:33.853749000 | 2023/09/13 22:37:33.85181500
TouristV.local | Local | ff02::1:3 | Local | 0 | 39 | 39 | 3.50 KB | 2023/09/13 22:22:33.853749000 | 2023/09/13 22:37:33.85170200
10.10.10.16 | Local | pki.goog | Google LLC,United S... | 4 | 0 | 127 | 15.27 KB | 2023/09/13 22:22:38.622863000 | 2023/09/13 22:37:54.20978400
10.10.10.16 | Local | 35.187.148.146 | Google LLC,Taipei,T... | 2 | 0 | 80 | 4.80 KB | 2023/09/13 22:22:41.388474000 | 2023/09/13 22:37:18.09938800
TouristV.local | Local | 239.255.255.250 | Local | 0 | 8 | 32 | 6.91 KB | 2023/09/13 22:22:53.913199000 | 2023/09/13 22:36:56.94737300
10.10.10.16 | Local | 142.251.222.195 | Google LLC,Mountai... | 1 | 0 | 27 | 1.62 KB | 2023/09/13 22:22:59.553971000 | 2023/09/13 22:32:23.82339200
8.8.8.8 | Google LLC,United S... | 10.10.10.16 | Local | 0 | 21 | 43 | 8.03 KB | 2023/09/13 22:23:00.321995000 | 2023/09/13 22:37:43.33090600
10.10.10.16 | Local | login.live.com | Microsoft Corporati... | 1 | 0 | 35 | 22.48 KB | 2023/09/13 22:23:00.395811000 | 2023/09/13 22:23:01.53899200
10.10.10.16 | Local | watson.telemetry.mi... | Microsoft Corporati... | 1 | 0 | 25 | 11.77 KB | 2023/09/13 22:23:01.728391000 | 2023/09/13 22:24:03.36036700
10.10.10.16 | Local | optimizationguide-... | Google LLC,United S... | 1 | 0 | 17 | 6.33 KB | 2023/09/13 22:23:25.289425000 | 2023/09/13 22:23:25.41421700
10.10.10.19 | Local | 20.189.79.72 | Microsoft Corporati... | 0 | 1 | 4 | 376.00 B | 2023/09/13 22:24:24.914617000 | 2023/09/13 22:32:56.99288000
TouristV.local | Local | 10.10.10.255 | Local | 0 | 1 | 3 | 288.00 B | 2023/09/13 22:24:27.835056000 | 2023/09/13 22:24:29.35273700
10.10.10.16 | Local | 20.198.118.190 | Microsoft Corporati... | 1 | 0 | 20 | 2.37 KB | 2023/09/13 22:24:59.014872000 | 2023/09/13 22:36:59.15620000
10.10.10.16 | Local | optimizationguide-... | Google LLC,Taipei,T... | 1 | 0 | 16 | 6.27 KB | 2023/09/13 22:26:47.927486000 | 2023/09/13 22:26:48.81088300
TCP Conversation
UDP Conversation
Log
TouristV.local <-> 224.0.0.22\TCP Conversation: 0
Node 1 -> | Port 1 -> | Endpoint 1 Geolocation-> | <- Node 2 | <- Port 2 | <-Endpoint 2 Geolocation | Protocol | Packets | Bytes | Payload | TCP State
There are no items to show in this view.
Capture - Default | Ethernet0 | Bandwidth - 1000Mbps | Inactive | 00:15:40 | 1,437 | 0 | Ready
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2016 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
Analysis Project 1 - Colasoft Capsa Enterprise Trial
File(F) Analysis Settings(N) Views(V) Tools(T) Resource(R) Product(P) Help(H)
Packets - 10.10.10.19 - 20.189.79.72 - Analysis Project 1
No. Date Absolute Time Source Source Port Source Geolocation Destination Destination Port Destination Geolocation Protocol Application
235 2023/09/13 22:24:24.914617000 10.10.10.19 123 Local 20.189.79.72 123 Microsoft Corporati... NTP
238 2023/09/13 22:24:24.948341000 20.189.79.72 123 Microsoft Corporati... 10.10.10.19 123 Local NTP
1014 2023/09/13 22:32:56.952195000 10.10.10.19 123 Local 20.189.79.72 123 Microsoft Corporati... NTP
1018 2023/09/13 22:32:56.992880000 20.189.79.72 123 Microsoft Corporati... 10.10.10.19 123 Local NTP
Packet Info
Number 235
Packet Length 94
Capture Length 90
Timestamp 2023/09/13 22:24:24.914617000
Ethernet - II [0/14]
Destination Address 00:50:56:EE:64:88 (VMware, Inc.) [0/6]
Source Address 00:0C:29:AC:81:BB (VMware, Inc.) [6/6]
Protocol Type 0x800 (IP) [12/2]
Internet Protocol [14/20]
Version 4 [14/1] 0xF0
Internet Header Length 5 (20) [14/1] 0x0F
Differentiated Services Field [15/1]
00000000 00 50 56 EE 64 88 00 0C 29 AC 81 BB 08 00 45 00 00 4C 5F BC 00
00000015 00 80 11 62 C3 0A 0A 0A 13 14 BD 4F 48 00 7B 00 7B 00 38 F3 3C
0000002A 1B 04 09 E9 00 00 0A 59 00 00 10 8B 14 BD 4F 48 E8 D5 29 B7 ED
0000003F 55 11 AA E8 D5 27 E8 D3 D8 2E 29 E8 D5 27 E8 DD 54 95 83 E8 D5
00000054 29 E8 D5 86 5F 2A
Original Packet
There are no items to show in this view.
Analysis Project 1 - Colasoft Capsa Enterprise Trial
Global - Top IP Group by Total Traffic (Packets)
Global - Top Local IP Address by Total Traffic (Packets)
Global - Top Remote IP Address by Total Traffic (Packets)
Local Subnet
Multicast Addresses
Link Local
Internet Addresses


V2016 - VMware Workstation
Analysis Project 1 - Colasoft Capsa Enterprise Trial
Top100 MAC Node(Matrix)
Top100 MAC Conversation
Top100 MAC Node
Top100 IP Conversation
Top100 IP Node
User Hidden Nodes (0)
Invisible Nodes (0)

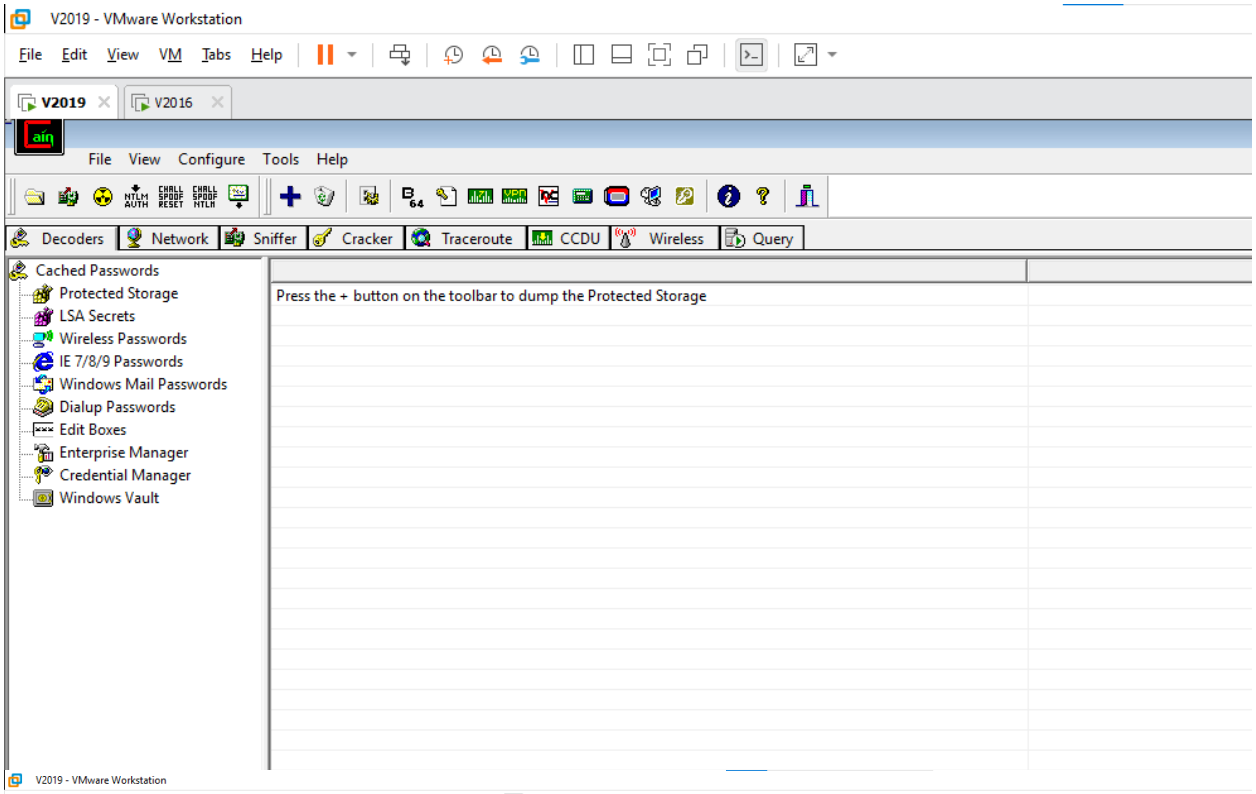

V2016 - VMware Workstation
Analysis Project 1 - Colasoft Capsa Enterprise Trial
Global Report
Creation Time: 2023/09/13 22:46:34
Traffic Statistics
Total Traffic Statistics
Packets Statistics
Packet Size Distribution Statistics
Broadcast Statistics
Multicast Statistics
Communication Statistics
Address Statistics
Conversation Statistics
Protocol Statistics
Diagnosis
Diagnosis Statistics
Top Address, Host and Domain
Top MAC Address by Total Traffic
Top MAC Address by Received Traffic
Top MAC Address by Sent Traffic
Top IP Address by Total Traffic
Top IP Address by Received Traffic
Top IP Address by Sent Traffic
Top IP Address Connection
Top Local IP Address by Total Traffic
Top Local IP Address by Received Traffic
Top Local IP Address by Sent Traffic
Top Local IP Address Connection
Top Remote IP Address by Total Traffic
Top Remote IP Address by Received Traffic
Top Remote IP Address by Sent Traffic
Top Domain Name
Top Conversation

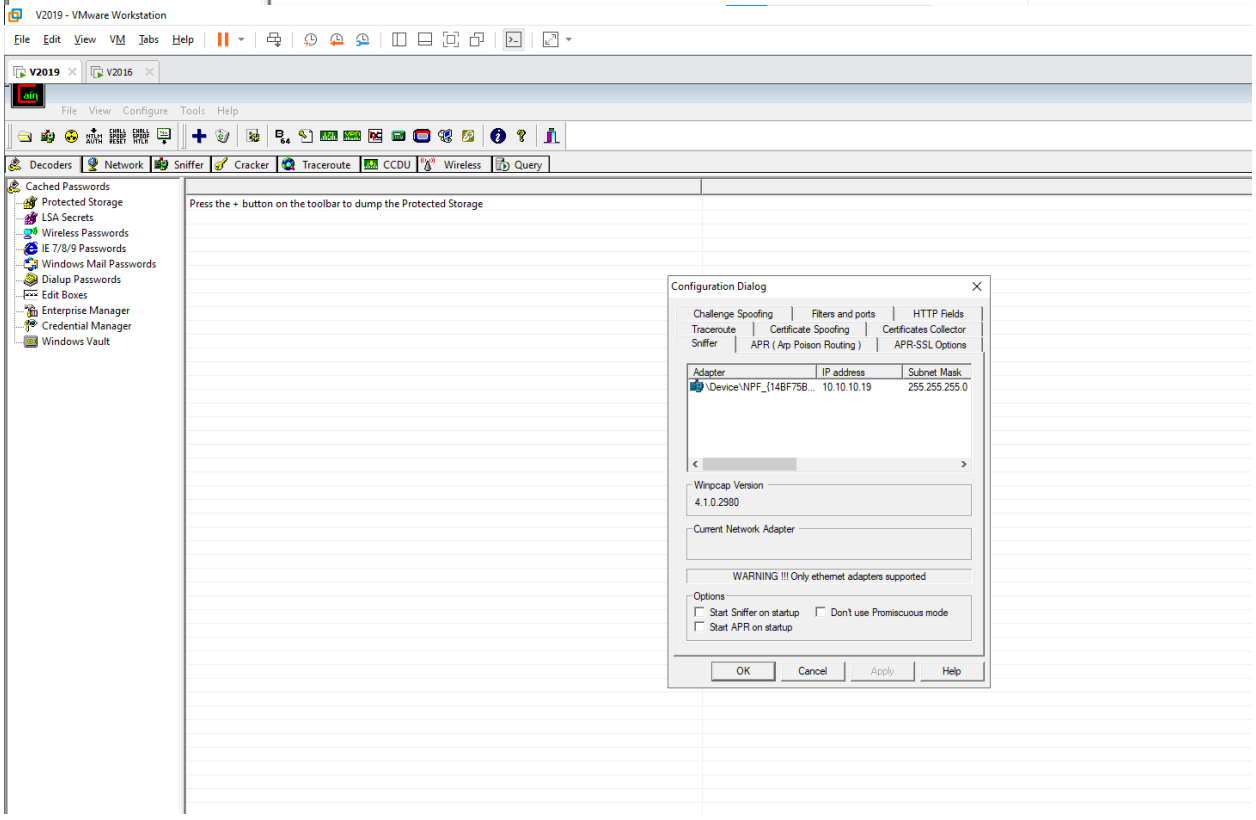


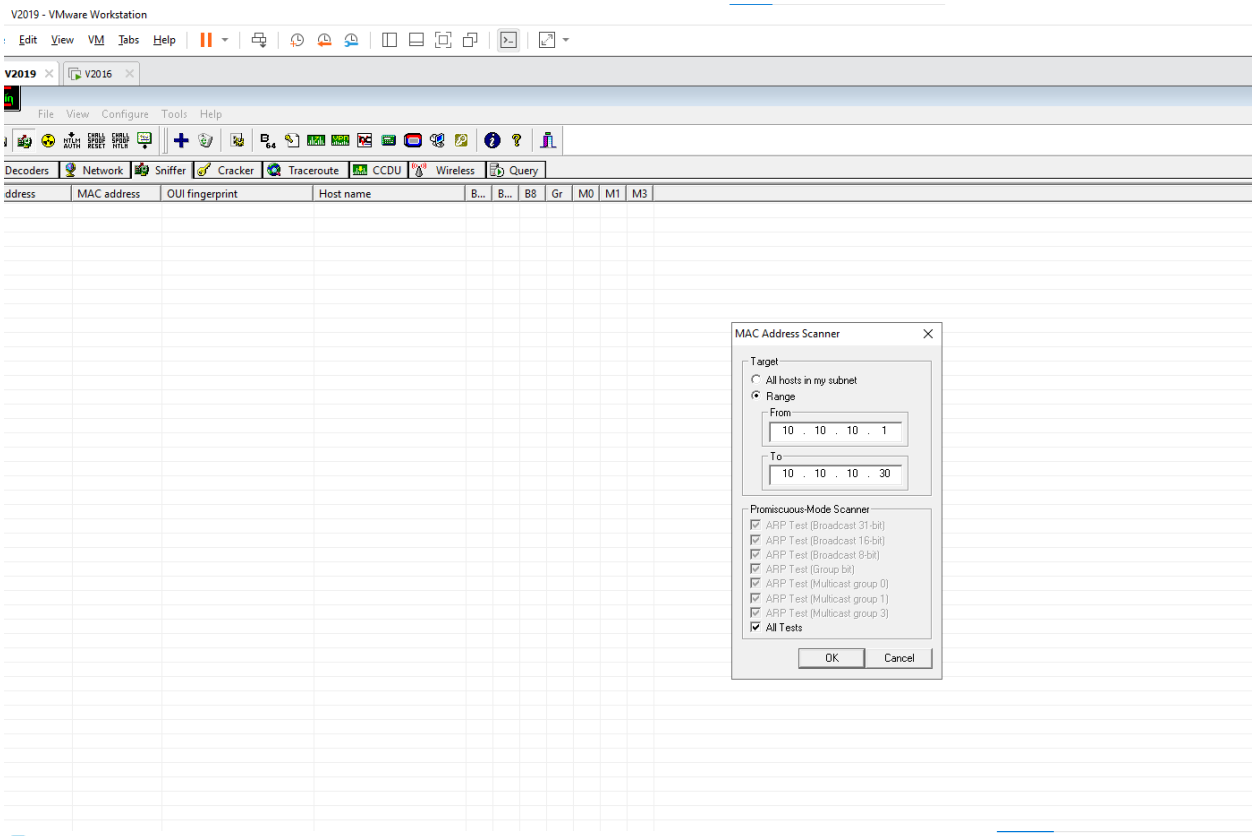
3. Detect Network Sniffing

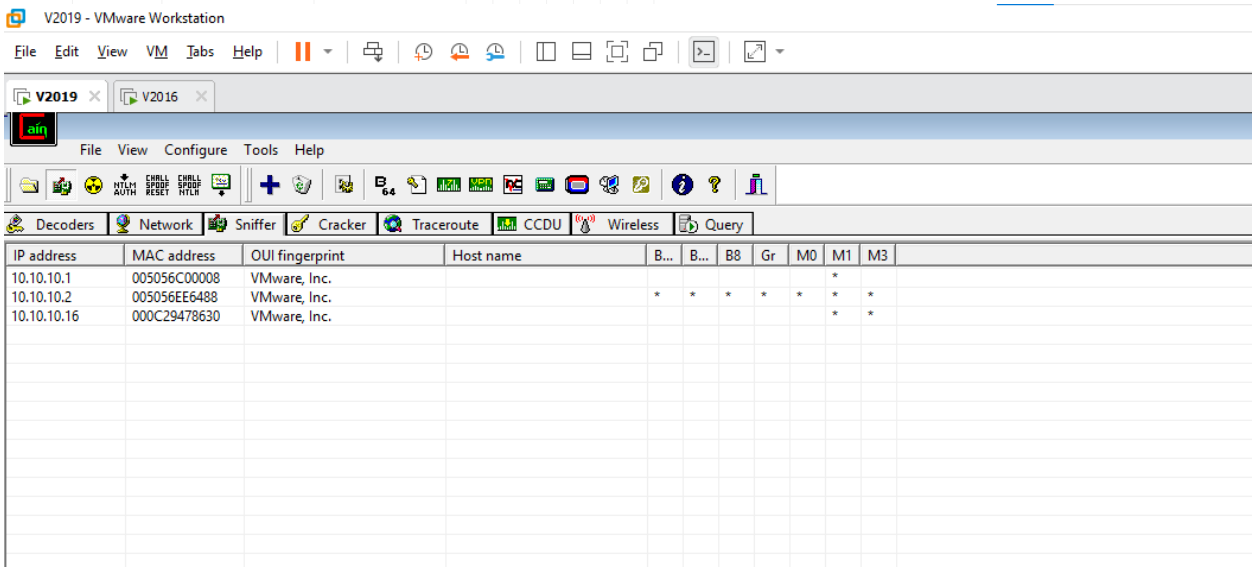
3.1 Detect ARP Poisoning in a Switch-Based Network

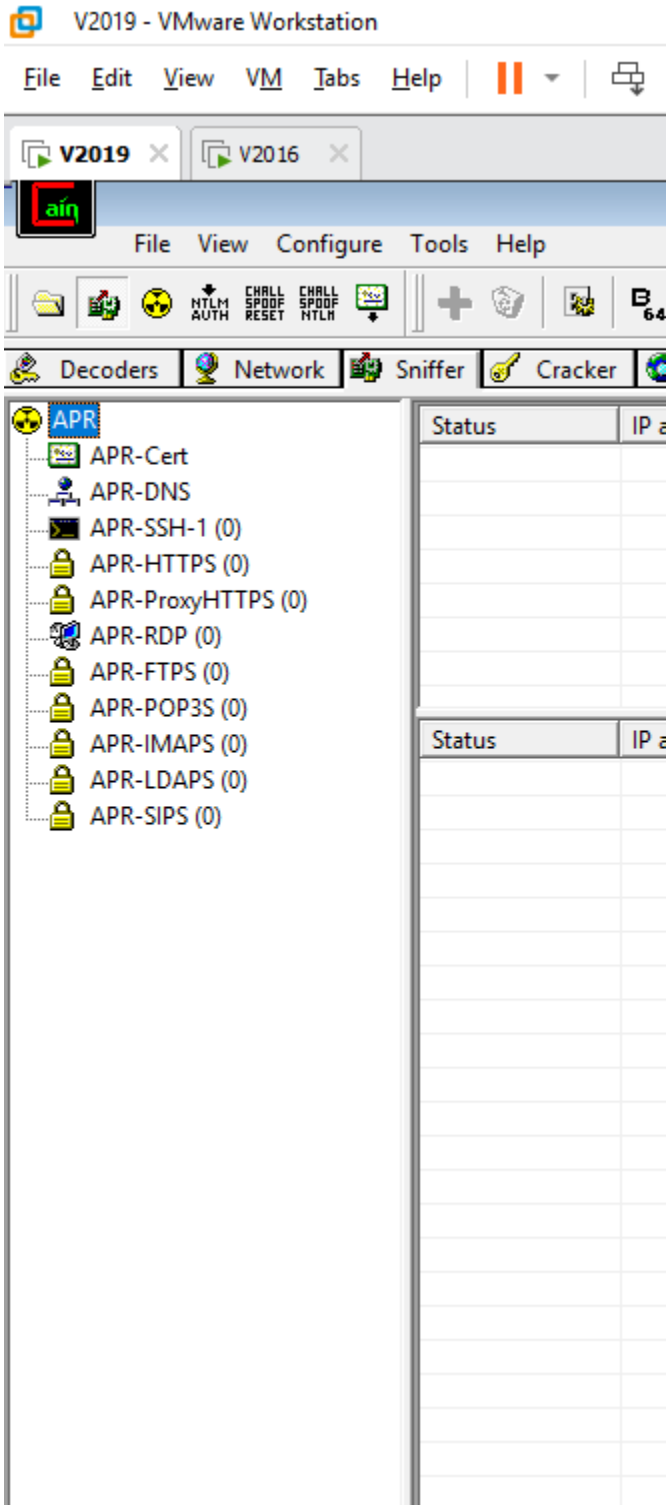
- Open Windows 10, Windows Server 2019, Parrot

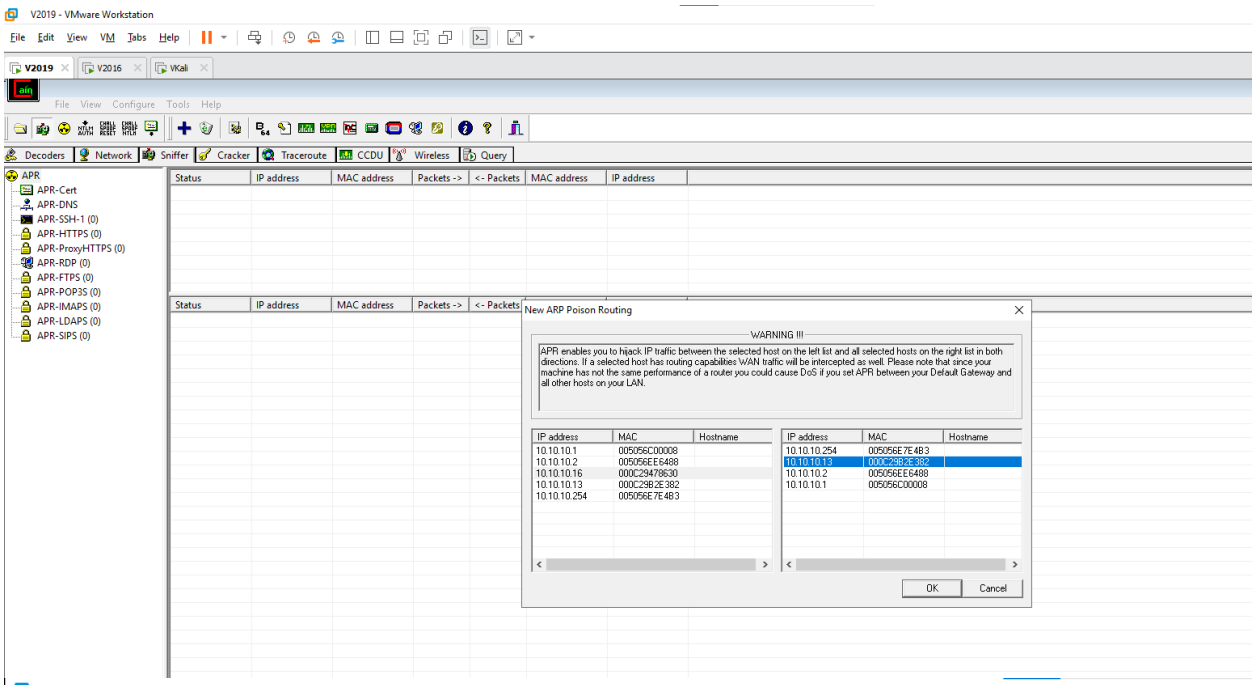

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE 7/8/9 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Windows Vault
Press the + button on the toolbar to dump the Protected Storage

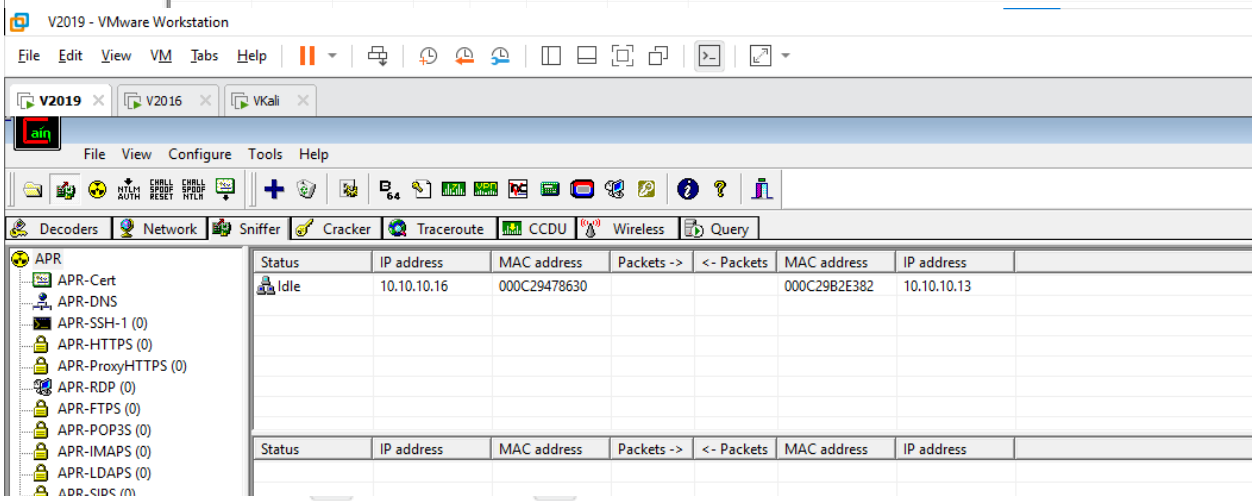

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE 7/8/9 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Windows Vault
Press the + button on the toolbar to dump the Protected Storage
Configuration Dialog
Challenge Spoofing
Filters and ports
HTTP Fields
Traceroute
Certificate Spoofing
Certificates Collector
Sniffer
APR (Arp Poison Routing)
APR-SSL Options
Adapter
IP address
Subnet Mask
\Device\NPF_{14BF75B... 10.10.10.19 255.255.255.0
Winpcap Version
4.1.0.2980
Current Network Adapter
WARNING !!! Only ethernet adapters supported
Options
Start Sniffer on startup
Don't use Promiscuous mode
Start APR on startup
OK
Cancel
Apply
Help

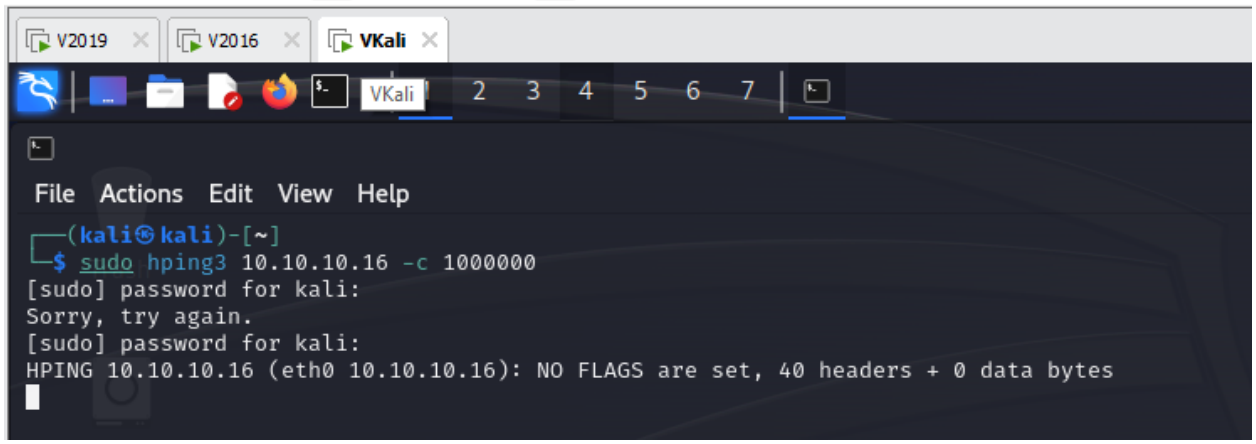

V2019 - VMware Workstation
Edit View VM Tabs Help
V2019
V2016
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
ddress MAC address OUI fingerprint Host name B... B... B8 Gr M0 M1 M3
MAC Address Scanner
Target
All hosts in my subnet
Range
From
10 . 10 . 10 . 1
To
10 . 10 . 10 . 30
Promiscuous-Mode Scanner
ARP Test (Broadcast 31-bit)
ARP Test (Broadcast 16-bit)
ARP Test (Broadcast 8-bit)
ARP Test (Group bit)
ARP Test (Multicast group 0)
ARP Test (Multicast group 1)
ARP Test (Multicast group 3)
All Tests
OK
Cancel

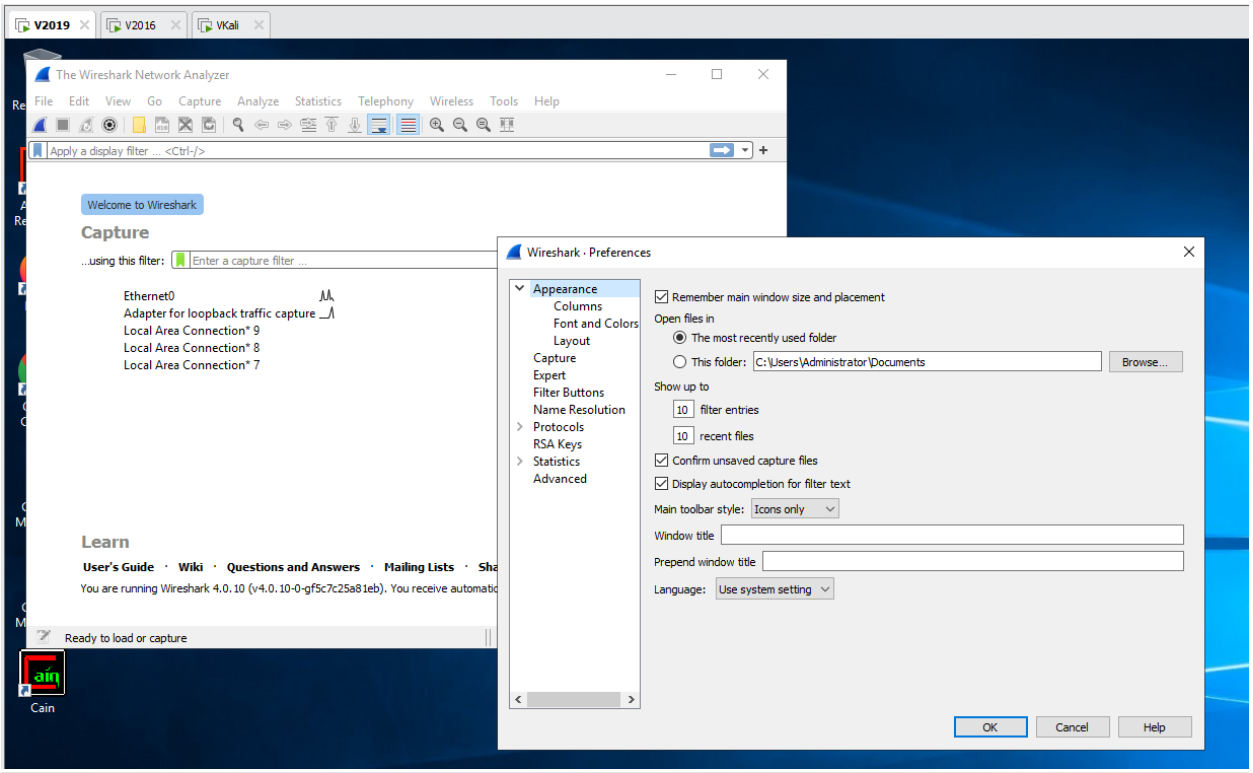

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B... B... B8 Gr M0 M1 M3
10.10.10.1 005056C00008 VMware, Inc. *
10.10.10.2 005056EE6488 VMware, Inc. * * * * * * *
10.10.10.16 000C29478630 VMware, Inc. * *

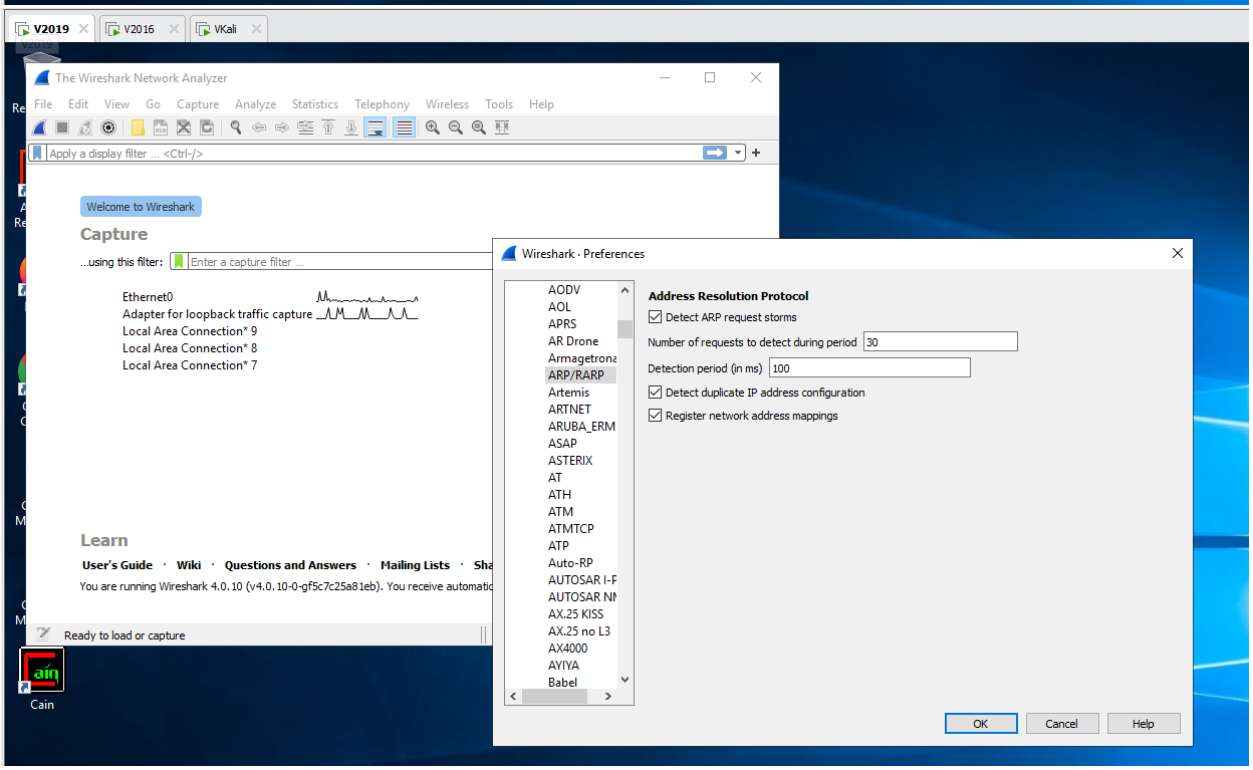

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP a
Status
IP a

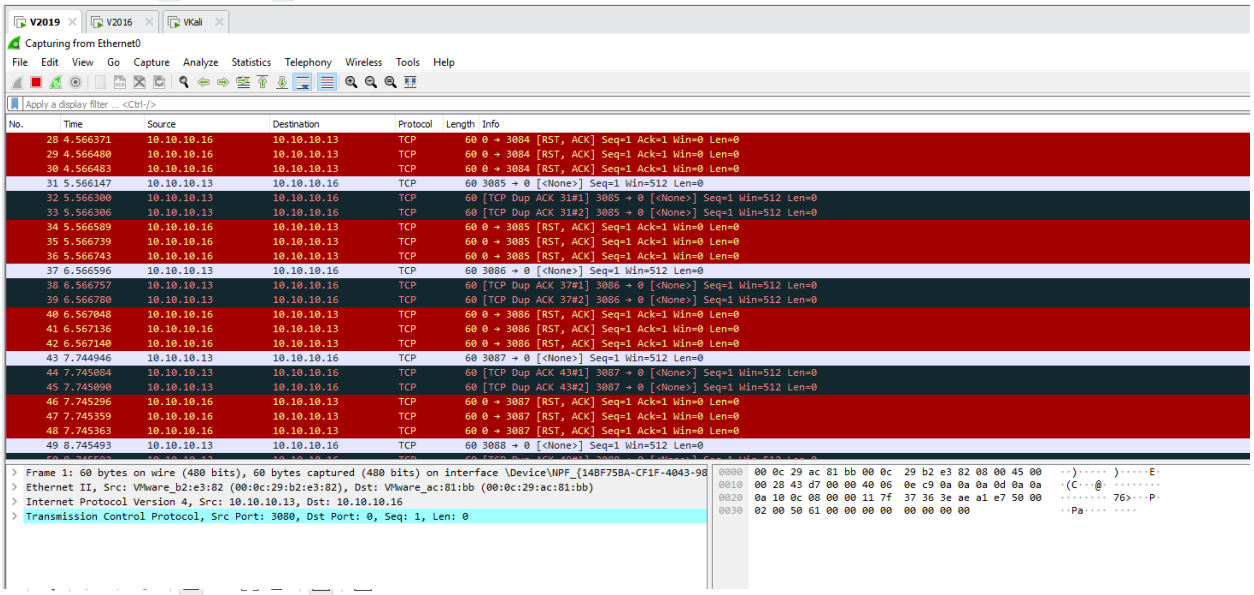

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
VKali
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
Hostname
10.10.10.1 005056C00008
10.10.10.2 005056EE6488
10.10.10.16 000C29478630
10.10.10.13 000C29B2E382
10.10.10.254 005056E7E4B3
OK
Cancel

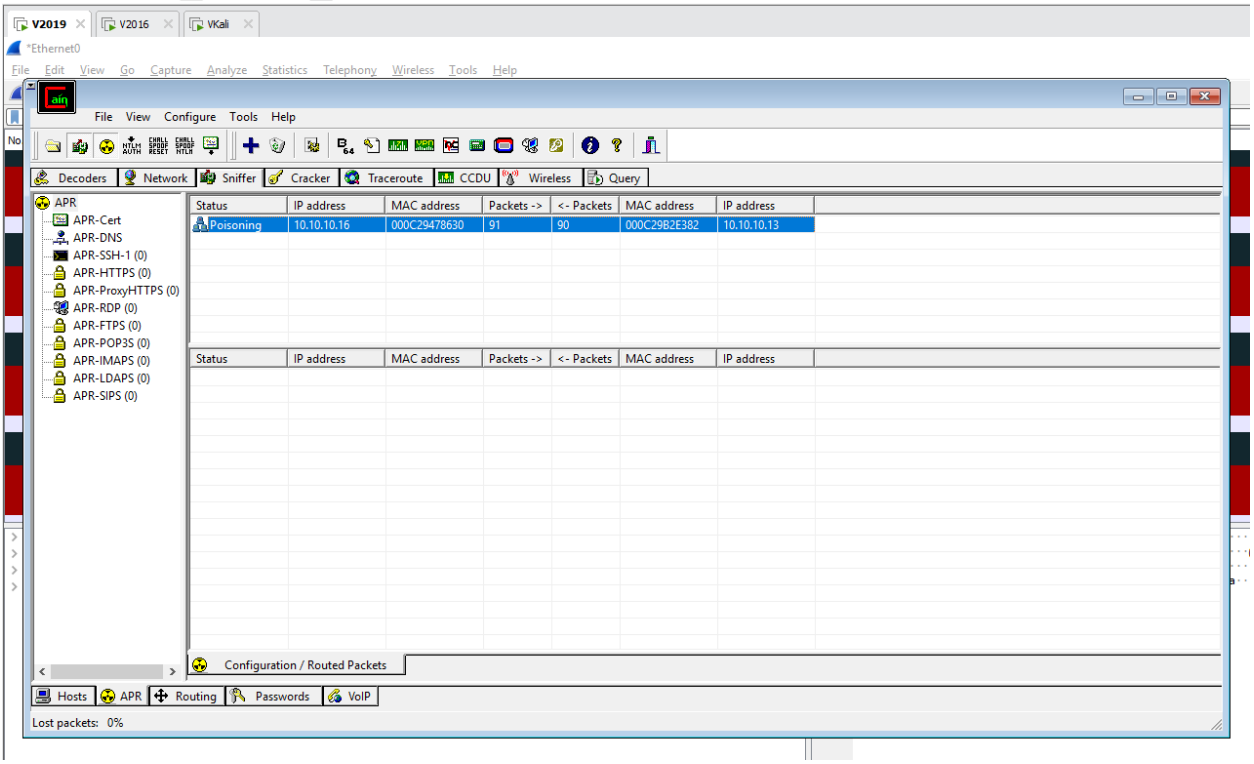

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2019
V2016
VKali
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
Status
IP address
MAC address
Packets ->
<- Packets
Idle
10.10.10.16
000C29478630
000C29B2E382
10.10.10.13

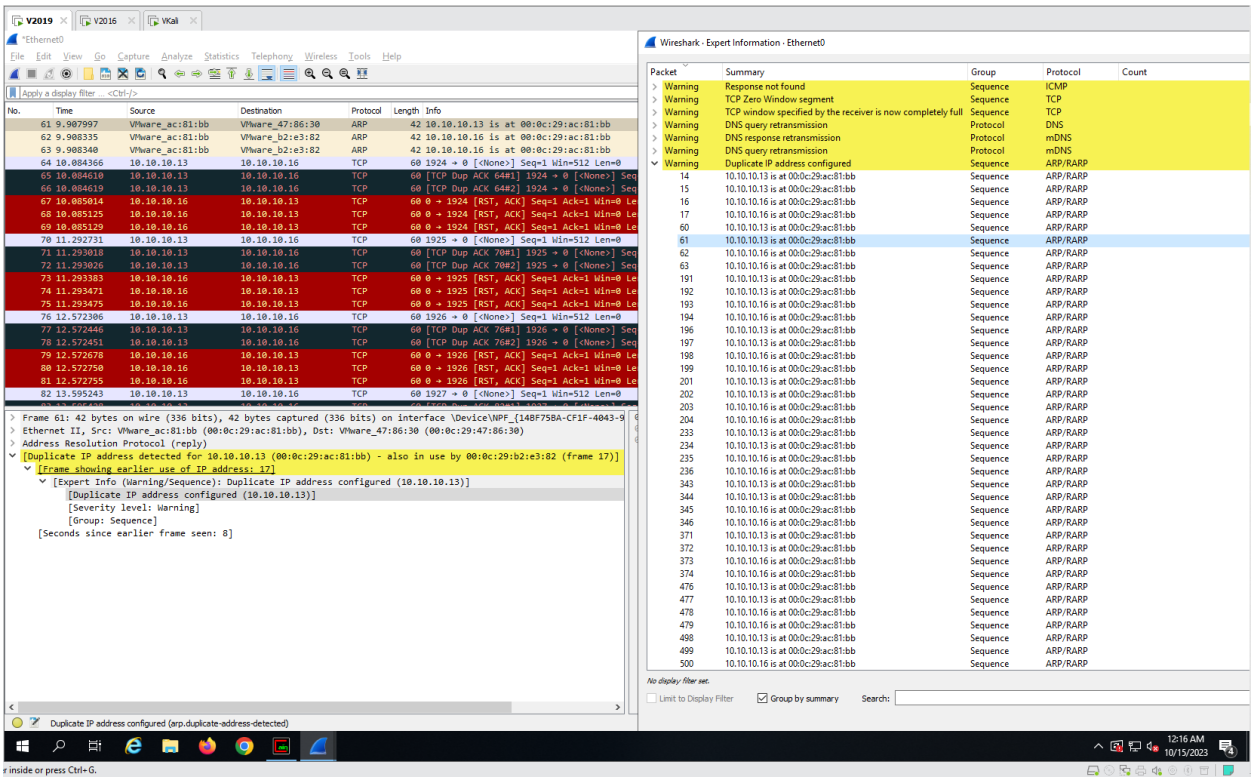

V2019
V2016
VKali
VKali
2
3
4
5
6
7
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo hping3 10.10.10.16 -c 1000000
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
HPING 10.10.10.16 (eth0 10.10.10.16): NO FLAGS are set, 40 headers + 0 data bytes

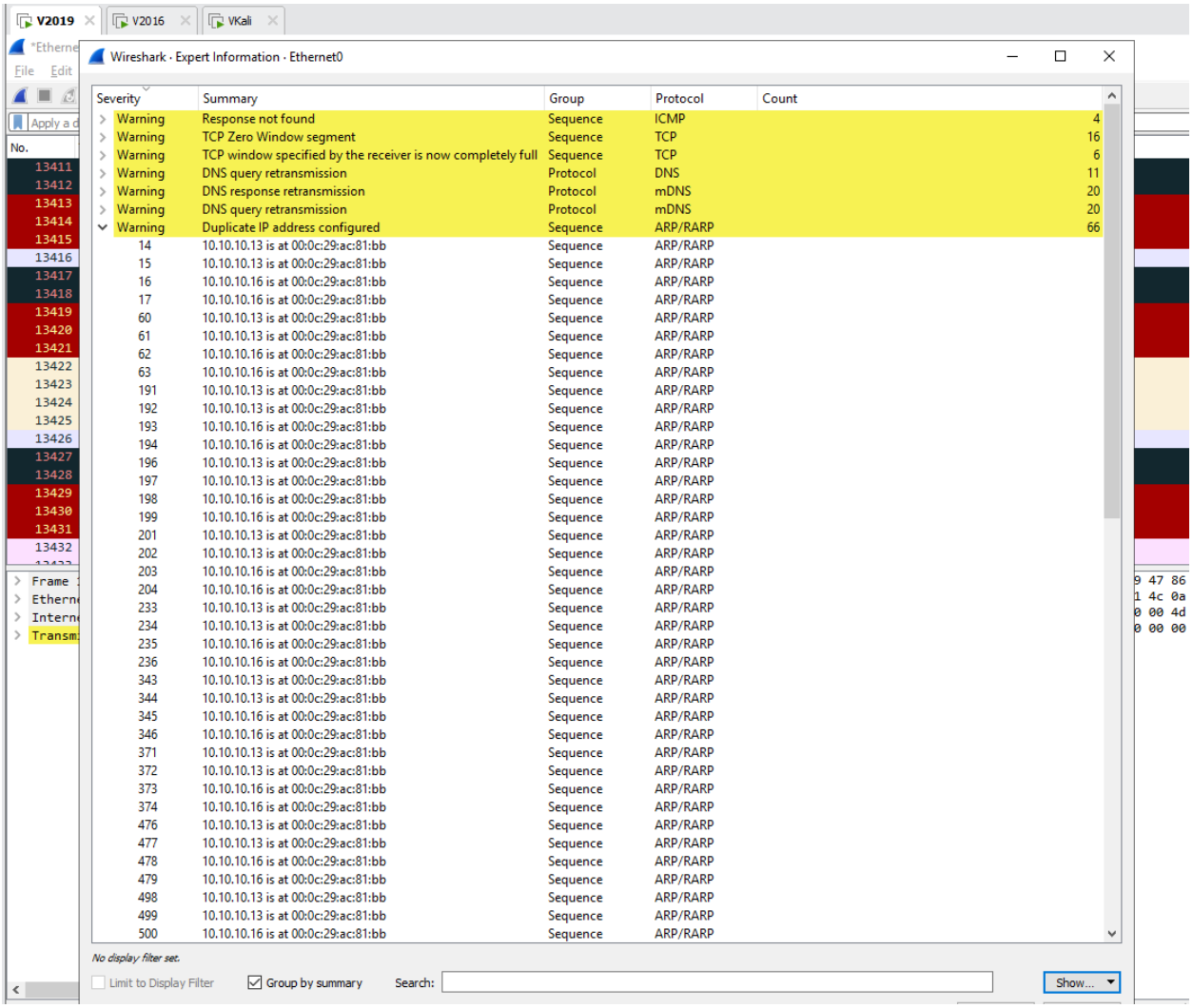

V2019
V2016
VKali
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
Ethernet0
Adapter for loopback traffic capture
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · Sha
You are running Wireshark 4.0.10 (v4.0.10-0-gf5c7c25a81eb). You receive automatic
Ready to load or capture
Cain
Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Remember main window size and placement
Open files in
The most recently used folder
This folder: C:\Users\Administrator\Documents
Browse...
Show up to
10 filter entries
10 recent files
Confirm unsaved capture files
Display autocompletion for filter text
Main toolbar style: Icons only
Window title
Prepend window title
Language: Use system setting
OK
Cancel
Help


V2019
V2016
VKali
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
Ethernet0
Adapter for loopback traffic capture
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · Sha
You are running Wireshark 4.0.10 (v4.0.10-0-gf5c7c25a81eb). You receive automatic
Ready to load or capture
Cain
Wireshark · Preferences
AODV
AOL
APRS
AR Drone
Armagetron
ARP/RARP
Artemis
ARTNET
ARUBA_ERM
ASAP
ASTERIX
AT
ATH
ATM
ATMTCP
ATP
Auto-RP
AUTOSAR I-P
AUTOSAR NM
AX.25 KISS
AX.25 no L3
AX4000
AYIYA
Babel
Address Resolution Protocol
Detect ARP request storms
Number of requests to detect during period 30
Detection period (in ms) 100
Detect duplicate IP address configuration
Register network address mappings
OK
Cancel
Help


V2019
V2016
VKali
Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
28 4.566371 10.10.10.16 10.10.10.13 TCP 60 0 → 3084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29 4.566480 10.10.10.16 10.10.10.13 TCP 60 0 → 3084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30 4.566483 10.10.10.16 10.10.10.13 TCP 60 0 → 3084 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31 5.566147 10.10.10.13 10.10.10.16 TCP 60 3085 → 0 [<None>] Seq=1 Win=512 Len=0
32 5.566300 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 31#1] 3085 → 0 [<None>] Seq=1 Win=512 Len=0
33 5.566306 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 31#2] 3085 → 0 [<None>] Seq=1 Win=512 Len=0
34 5.566589 10.10.10.16 10.10.10.13 TCP 60 0 → 3085 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35 5.566739 10.10.10.16 10.10.10.13 TCP 60 0 → 3085 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36 5.566743 10.10.10.16 10.10.10.13 TCP 60 0 → 3085 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
37 6.566596 10.10.10.13 10.10.10.16 TCP 60 3086 → 0 [<None>] Seq=1 Win=512 Len=0
38 6.566757 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 37#1] 3086 → 0 [<None>] Seq=1 Win=512 Len=0
39 6.566780 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 37#2] 3086 → 0 [<None>] Seq=1 Win=512 Len=0
40 6.567048 10.10.10.16 10.10.10.13 TCP 60 0 → 3086 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 6.567136 10.10.10.16 10.10.10.13 TCP 60 0 → 3086 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
42 6.567140 10.10.10.16 10.10.10.13 TCP 60 0 → 3086 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43 7.744946 10.10.10.13 10.10.10.16 TCP 60 3087 → 0 [<None>] Seq=1 Win=512 Len=0
44 7.745084 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 43#1] 3087 → 0 [<None>] Seq=1 Win=512 Len=0
45 7.745090 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 43#2] 3087 → 0 [<None>] Seq=1 Win=512 Len=0
46 7.745296 10.10.10.16 10.10.10.13 TCP 60 0 → 3087 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47 7.745359 10.10.10.16 10.10.10.13 TCP 60 0 → 3087 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48 7.745363 10.10.10.16 10.10.10.13 TCP 60 0 → 3087 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 8.745493 10.10.10.13 10.10.10.16 TCP 60 3088 → 0 [<None>] Seq=1 Win=512 Len=0
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{14BF75BA-CF1F-4043-98
Ethernet II, Src: VMware_b2:e3:82 (00:0c:29:b2:e3:82), Dst: VMware_ac:81:bb (00:0c:29:ac:81:bb)
Internet Protocol Version 4, Src: 10.10.10.13, Dst: 10.10.10.16
Transmission Control Protocol, Src Port: 3080, Dst Port: 0, Seq: 1, Len: 0
0000 00 0c 29 ac 81 bb 00 0c 29 b2 e3 82 08 00 45 00
0010 00 28 43 d7 00 00 40 06 0e c9 0a 0a 0a 0d 0a 0a
0020 0a 10 0c 08 00 00 11 7f 37 36 3e ae a1 e7 50 00
0030 02 00 50 61 00 00 00 00 00 00 00 00

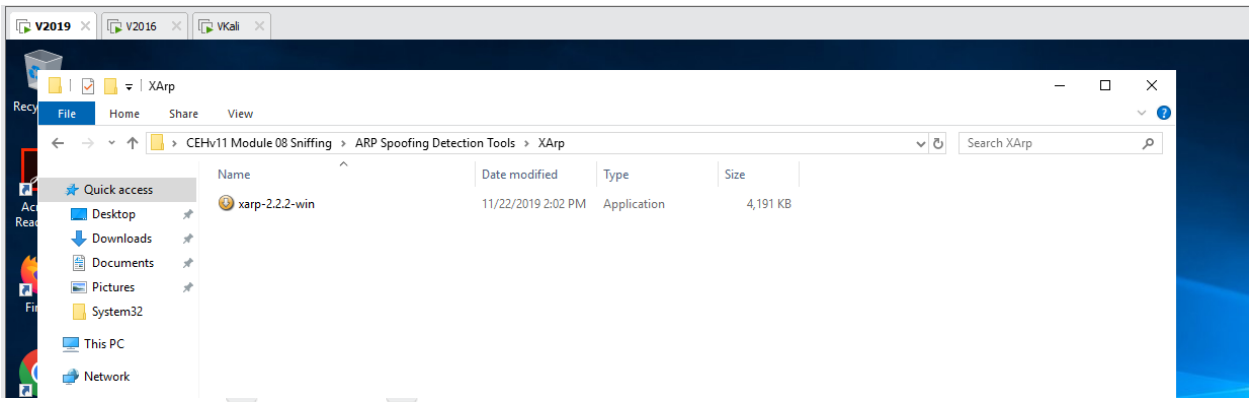

V2019
V2016
VKali
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 10.10.10.16 000C29478630 91 90 000C29B2E382 10.10.10.13
Status IP address MAC address Packets -> <- Packets MAC address IP address
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

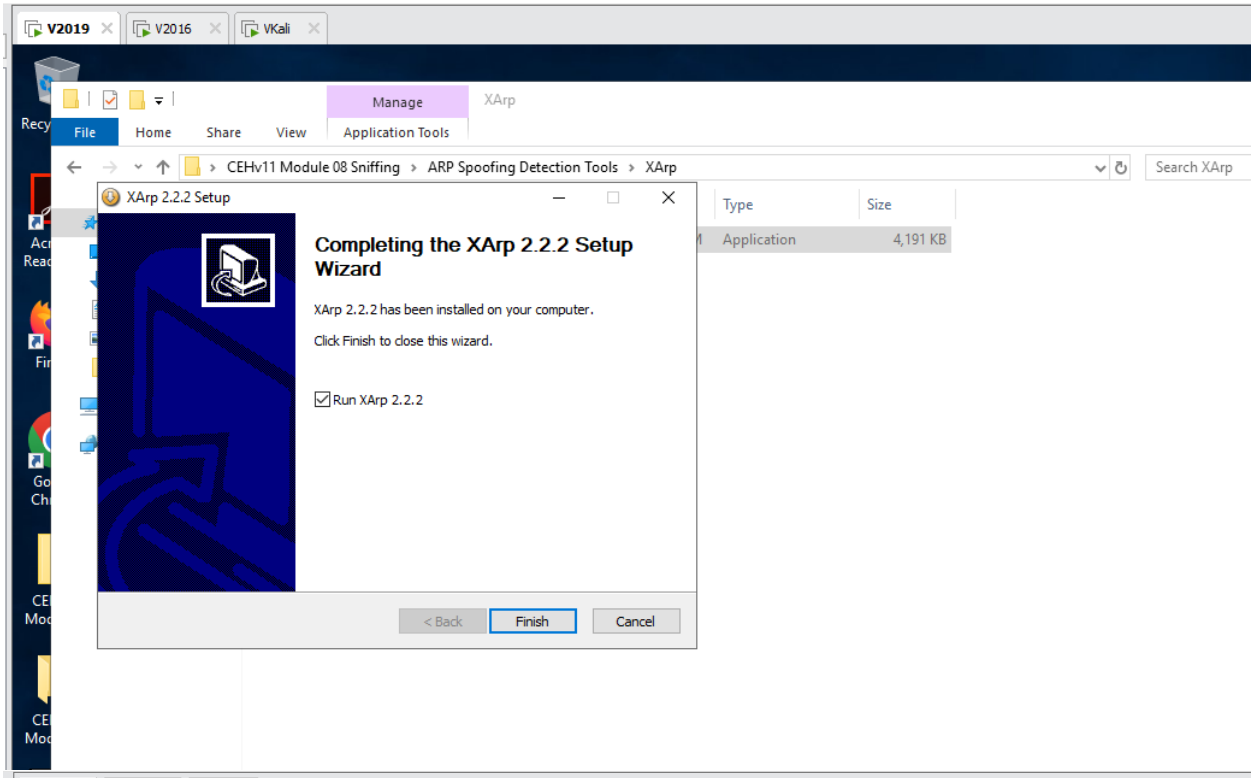

V2019
V2016
VKali
*Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
61 9.907997 VMware_ac:81:bb VMware_47:86:30 ARP 42 10.10.10.13 is at 00:0c:29:ac:81:bb
62 9.908335 VMware_ac:81:bb VMware_b2:e3:82 ARP 42 10.10.10.16 is at 00:0c:29:ac:81:bb
63 9.908340 VMware_ac:81:bb VMware_b2:e3:82 ARP 42 10.10.10.16 is at 00:0c:29:ac:81:bb
64 10.004366 10.10.10.13 10.10.10.16 TCP 60 1924 → 0 [<None>] Seq=1 Win=512 Len=0
65 10.004610 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 64#1] 1924 → 0 [<None>] Seq
66 10.004619 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 64#2] 1924 → 0 [<None>] Seq
67 10.085014 10.10.10.16 10.10.10.13 TCP 60 0 → 1924 [RST, ACK] Seq=1 Ack=1 Win=0 Le
68 10.085125 10.10.10.16 10.10.10.13 TCP 60 0 → 1924 [RST, ACK] Seq=1 Ack=1 Win=0 Le
69 10.085129 10.10.10.16 10.10.10.13 TCP 60 0 → 1924 [RST, ACK] Seq=1 Ack=1 Win=0 Le
70 11.292731 10.10.10.13 10.10.10.16 TCP 60 1925 → 0 [<None>] Seq=1 Win=512 Len=0
71 11.293018 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 70#1] 1925 → 0 [<None>] Seq
72 11.293026 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 70#2] 1925 → 0 [<None>] Seq
73 11.293383 10.10.10.16 10.10.10.13 TCP 60 0 → 1925 [RST, ACK] Seq=1 Ack=1 Win=0 Le
74 11.293471 10.10.10.16 10.10.10.13 TCP 60 0 → 1925 [RST, ACK] Seq=1 Ack=1 Win=0 Le
75 11.293475 10.10.10.16 10.10.10.13 TCP 60 0 → 1925 [RST, ACK] Seq=1 Ack=1 Win=0 Le
76 12.572306 10.10.10.13 10.10.10.16 TCP 60 1926 → 0 [<None>] Seq=1 Win=512 Len=0
77 12.572446 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 76#1] 1926 → 0 [<None>] Seq
78 12.572451 10.10.10.13 10.10.10.16 TCP 60 [TCP Dup ACK 76#2] 1926 → 0 [<None>] Seq
79 12.572678 10.10.10.16 10.10.10.13 TCP 60 0 → 1926 [RST, ACK] Seq=1 Ack=1 Win=0 Le
80 12.572750 10.10.10.16 10.10.10.13 TCP 60 0 → 1926 [RST, ACK] Seq=1 Ack=1 Win=0 Le
81 12.572755 10.10.10.16 10.10.10.13 TCP 60 0 → 1926 [RST, ACK] Seq=1 Ack=1 Win=0 Le
82 13.595243 10.10.10.13 10.10.10.16 TCP 60 1927 → 0 [<None>] Seq=1 Win=512 Len=0
Frame 61: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{14BF75BA-CF1F-4043-9
Ethernet II, Src: VMware_ac:81:bb (00:0c:29:ac:81:bb), Dst: VMware_47:86:30 (00:0c:29:47:86:30)
Address Resolution Protocol (reply)
[Duplicate IP address detected for 10.10.10.13 (00:0c:29:ac:81:bb) - also in use by 00:0c:29:b2:e3:82 (frame 17)]
[Frame showing earlier use of IP address: 17]
[Expert Info (Warning/Sequence): Duplicate IP address configured (10.10.10.13)]
[Duplicate IP address configured (10.10.10.13)]
[Severity level: Warning]
[Group: Sequence]
[Seconds since earlier frame seen: 8]
Duplicate IP address configured (arp.duplicate-address-detected)
Wireshark · Expert Information · Ethernet0
Packet Summary Group Protocol Count
Warning Response not found Sequence ICMP
Warning TCP Zero Window segment Sequence TCP
Warning TCP window specified by the receiver is now completely full Sequence TCP
Warning DNS query retransmission Protocol DNS
Warning DNS response retransmission Protocol mDNS
Warning DNS query retransmission Protocol mDNS
Warning Duplicate IP address configured Sequence ARP/RARP
14 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
15 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
16 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
17 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
60 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
61 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
62 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
63 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
191 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
192 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
193 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
194 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
196 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
197 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
198 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
199 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
201 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
202 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
203 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
204 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
233 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
234 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
235 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
236 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
343 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
344 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
345 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
346 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
371 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
372 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
373 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
374 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
476 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
477 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
478 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
479 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
498 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
499 10.10.10.13 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
500 10.10.10.16 is at 00:0c:29:ac:81:bb Sequence ARP/RARP
No display filter set.
Limit to Display Filter
Group by summary
Search:
12:16 AM
10/15/2023
r inside or press Ctrl+G.

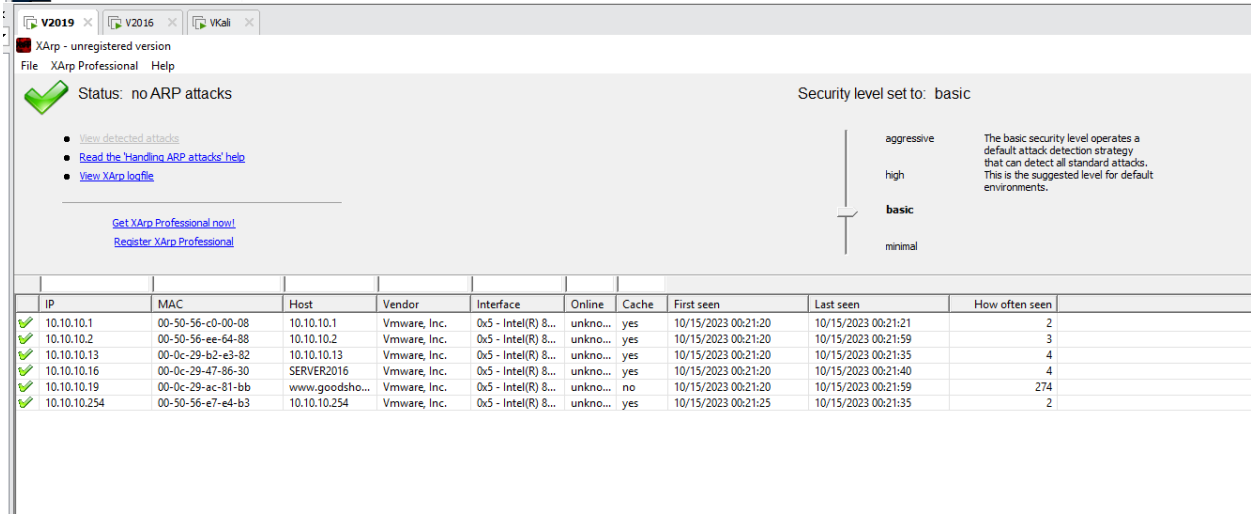


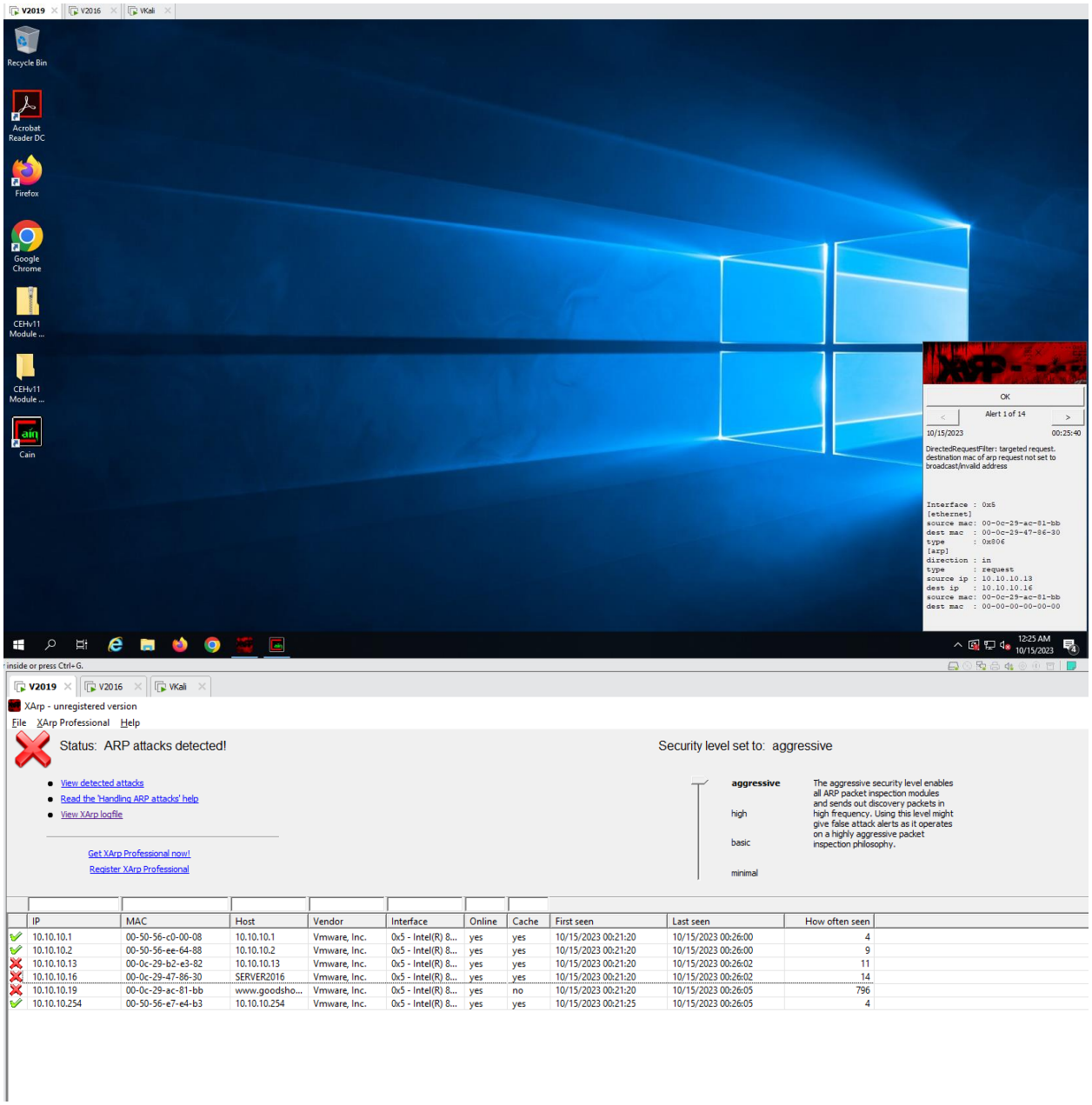
3.2 Detect ARP Attacks using Xarp

- Open Windows 10, Windows Server 2019, Parrot


V2019
V2016
VKali
XArp
File
Home
Share
View
CEHv11 Module 08 Sniffing › ARP Spoofing Detection Tools › XArp
Search XArp
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
xarp-2.2.2-win
11/22/2019 2:02 PM
Application
4,191 KB

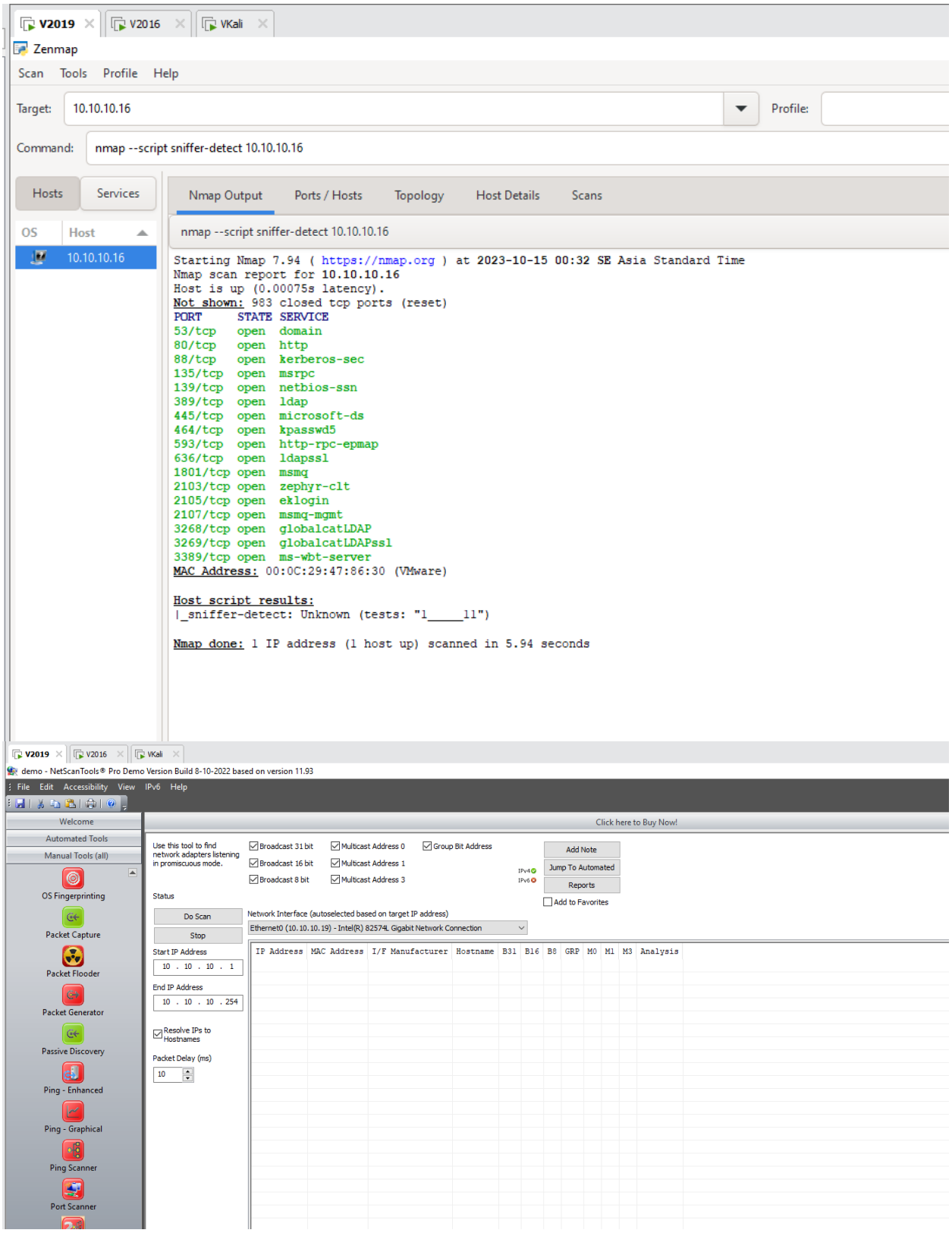

V2019
V2016
VKali
Manage
XArp
File
Home
Share
View
Application Tools
CEHv11 Module 08 Sniffing › ARP Spoofing Detection Tools › XArp
Search XArp
Type
Size
Application
4,191 KB
XArp 2.2.2 Setup
Completing the XArp 2.2.2 Setup Wizard
XArp 2.2.2 has been installed on your computer.
Click Finish to close this wizard.
Run XArp 2.2.2
< Back
Finish
Cancel

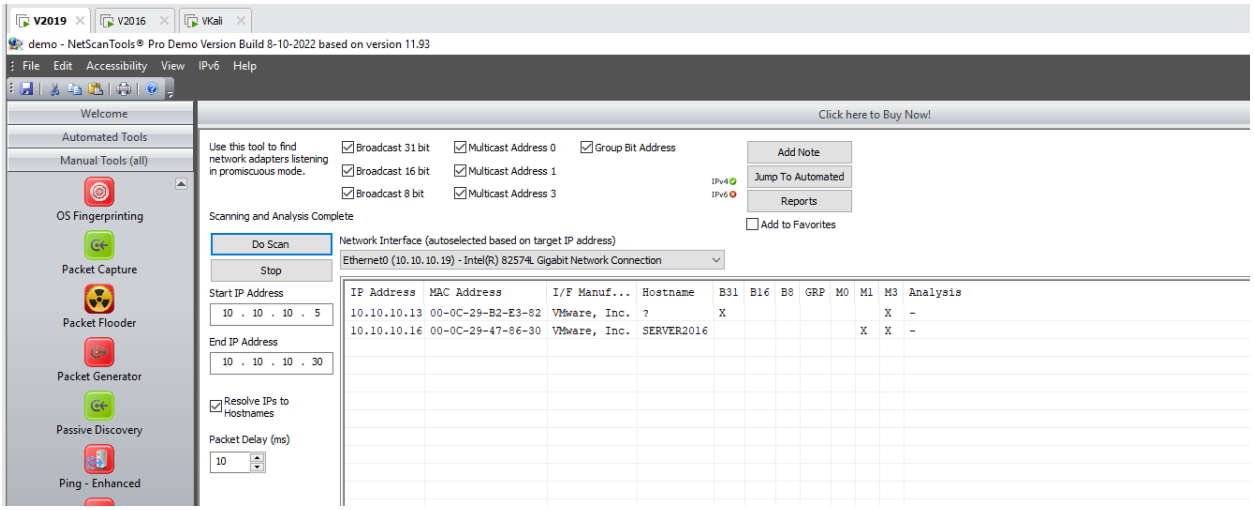

V2019
V2016
VKali
XArp - unregistered version
File
XArp Professional
Help
Status: no ARP attacks
View detected attacks
Read the 'Handling ARP attacks' help
View XArp logfile
Get XArp Professional now!
Register XArp Professional
Security level set to: basic
aggressive
high
basic
minimal
The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.
IP
MAC
Host
Vendor
Interface
Online
Cache
First seen
Last seen
How often seen
10.10.10.1 00-50-56-c0-00-08 10.10.10.1 Vmware, Inc. 0x5 - Intel(R) 8... unkno... yes 10/15/2023 00:21:20 10/15/2023 00:21:21 2
10.10.10.2 00-50-56-ee-64-88 10.10.10.2 Vmware, Inc. 0x5 - Intel(R) 8... unkno... yes 10/15/2023 00:21:20 10/15/2023 00:21:59 3
10.10.10.13 00-0c-29-b2-e3-82 10.10.10.13 Vmware, Inc. 0x5 - Intel(R) 8... unkno... yes 10/15/2023 00:21:20 10/15/2023 00:21:35 4
10.10.10.16 00-0c-29-47-86-30 SERVER2016 Vmware, Inc. 0x5 - Intel(R) 8... unkno... yes 10/15/2023 00:21:20 10/15/2023 00:21:40 4
10.10.10.19 00-0c-29-ac-81-bb www.goodsho... Vmware, Inc. 0x5 - Intel(R) 8... unkno... no 10/15/2023 00:21:20 10/15/2023 00:21:59 274
10.10.10.254 00-50-56-e7-e4-b3 10.10.10.254 Vmware, Inc. 0x5 - Intel(R) 8... unkno... yes 10/15/2023 00:21:25 10/15/2023 00:21:35 2



3.3 Detect Promiscuous Mode using Nmap and NetScan Tools Pro

- Open Windows 10, Windows Server 2019, Parrot


V2019
V2016
VKali
Zenmap
Scan Tools Profile Help
Target: 10.10.10.16
Profile:
Command: nmap --script sniffer-detect 10.10.10.16
Hosts Services
OS Host
10.10.10.16
Nmap Output Ports / Hosts Topology Host Details Scans
nmap --script sniffer-detect 10.10.10.16
Starting Nmap 7.94 (https://nmap.org) at 2023-10-15 00:32 SE Asia Standard Time
Nmap scan report for 10.10.10.16
Host is up (0.00075s latency).
Not shown: 983 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
80/tcp open http
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
1801/tcp open msmq
2103/tcp open zephyr-clt
2105/tcp open eklogin
2107/tcp open msmq-mgmt
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
3389/tcp open ms-wbt-server
MAC Address: 00:0C:29:47:86:30 (VMware)
Host script results:
|_sniffer-detect: Unknown (tests: "1_____11")
Nmap done: 1 IP address (1 host up) scanned in 5.94 seconds
V2019
V2016
VKali
demo - NetScanTools® Pro Demo Version Build 8-10-2022 based on version 11.93
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
OS Fingerprinting
Packet Capture
Packet Flooder
Packet Generator
Passive Discovery
Ping - Enhanced
Ping - Graphical
Ping Scanner
Port Scanner
Click here to Buy Now!
Use this tool to find network adapters listening in promiscuous mode.
Broadcast 31 bit
Broadcast 16 bit
Broadcast 8 bit
Multicast Address 0
Multicast Address 1
Multicast Address 3
Group Bit Address
Add Note
Jump To Automated
Reports
Add to Favorites
Status
Do Scan
Stop
Network Interface (autoselected based on target IP address)
Ethernet0 (10.10.10.19) - Intel(R) 82574L Gigabit Network Connection
Start IP Address
10 . 10 . 10 . 1
End IP Address
10 . 10 . 10 . 254
Resolve IPs to Hostnames
Packet Delay (ms)
10
IP Address MAC Address I/F Manufacturer Hostname B31 B16 B8 GRP M0 M1 M3 Analysis


V2019
V2016
VKali
demo - NetScanTools® Pro Demo Version Build 8-10-2022 based on version 11.93
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
OS Fingerprinting
Packet Capture
Packet Flooder
Packet Generator
Passive Discovery
Ping - Enhanced
Click here to Buy Now!
Use this tool to find network adapters listening in promiscuous mode.
Broadcast 31 bit
Broadcast 16 bit
Broadcast 8 bit
Multicast Address 0
Multicast Address 1
Multicast Address 3
Group Bit Address
Add Note
Jump To Automated
Reports
Add to Favorites
Scanning and Analysis Complete
Do Scan
Stop
Network Interface (autoselected based on target IP address)
Ethernet0 (10.10.10.19) - Intel(R) 82574L Gigabit Network Connection
Start IP Address
10 . 10 . 10 . 5
End IP Address
10 . 10 . 10 . 30
Resolve IPs to Hostnames
Packet Delay (ms)
10
IP Address MAC Address I/F Manuf... Hostname B31 B16 B8 GRP M0 M1 M3 Analysis
10.10.10.13 00-0C-29-B2-E3-82 VMware, Inc. ? X X -
10.10.10.16 00-0C-29-47-86-30 VMware, Inc. SERVER2016 X X -