Cold as Ice: Answers to Unit 42 Wireshark Quiz for IcedID

unit42.paloaltonetworks.com/wireshark-quiz-icedid-answers/

Brad Duncan May 30, 2023

By Brad Duncan

May 30, 2023 at 6:00 AM

Category: Tutorial

Tags: Advanced Threat Prevention, Advanced URL Filtering, banking trojans, BokBot, Cloud-Delivered Security Services, Cortex XDR, IcedID, next-generation firewall, pcap, WildFire, Wireshark, Wireshark Tutorial

This post is also available in: 日本語 (Japanese)

Executive Summary

Our introductory blog Cold as Ice: Unit 42 Wireshark Quiz for IcedID provides a packet capture (pcap) from an IcedID infection in April 2023. This blog provides the answers. Also known as Bokbot, IcedID is well-established Windows-based malware that can lead to ransomware. Reviewing the pcap provides an opportunity to analyze IcedID infection traffic.

If you would like to view this quiz without answers, please see our previous blog introducing the standalone quiz.

Palo Alto Networks customers are protected from IcedID and other malware through Cortex XDR and our Next-Generation Firewall with Cloud-Delivered Security Services that include WildFire, Advanced Threat Prevention and Advanced URL Filtering.

Related Unit 42 Topics **pcap,Wireshark, Wireshark Tutorial, IcedID, BokBot**

Table of Contents

Scenario, Requirements and Quiz Material

Traffic for this quiz occurred in an Active Directory (AD) environment during April 2023. The infection is similar to previous IcedID activity tweeted by Unit 42 in March 2023. Details of the Local Area Network (LAN) environment for the pcap follow.

- LAN segment range: 10.4.19[.]0/24 (10.4.19[.]1 through 10.4.19[.]255)
- Domain: boogienights[.]live
- Domain controller IP address: 10.4.19[.]19
- Domain controller hostname: WIN-GP4JHCK2JMV
- LAN segment gateway: 10.4.19[.]1
- LAN segment broadcast address: 10.4.19[.]255

This quiz requires Wireshark, and we recommend using the latest version of Wireshark, since it has more features, capabilities and bug fixes over previous versions.

We also recommend readers customize their Wireshark display to better analyze web traffic. A list of tutorials and videos is available. As always, we recommend using Wireshark in a non-Windows environment like BSD, Linux or macOS when analyzing malicious Windows-based traffic.

To obtain the pcap, visit our GitHub repository, download the April 2023 ZIP archive and extract the pcap. Use *infected* as the password to unlock the ZIP archive.

Quiz Questions

For this IcedID infection, we ask participants to answer the following questions previously described in our standalone quiz post:

- What is the date and time in UTC the infection started?
- What is the IP address of the infected Windows client?
- What is the MAC address of the infected Windows client?
- What is the hostname of the infected Windows client?
- What is the user account name from the infected Windows host?
- Is there any follow-up activity from other malware?

Quiz Answers

The AD environment for this pcap contains three Windows clients, but only one was infected with IcedID.

Answers for this Wireshark quiz follow.

- Malicious traffic for this infection started on April 19, 2023, at 15:31 UTC.
- Infected Windows client IP address: 10.4.19[.]136
- Infected Windows client MAC address: 14:58:d0:2e:c5:ae
- Infected Windows client hostname: DESKTOP-SFF9LJF
- Infected Windows client user account name: csilva
- Follow-up activity: BackConnect traffic

Pcap Analysis: IcedID Chain of Events

To understand IcedID network traffic, you should understand the chain of events for an IcedID infection. A flow chart illustrating this chain of events is shown in Figure 1.

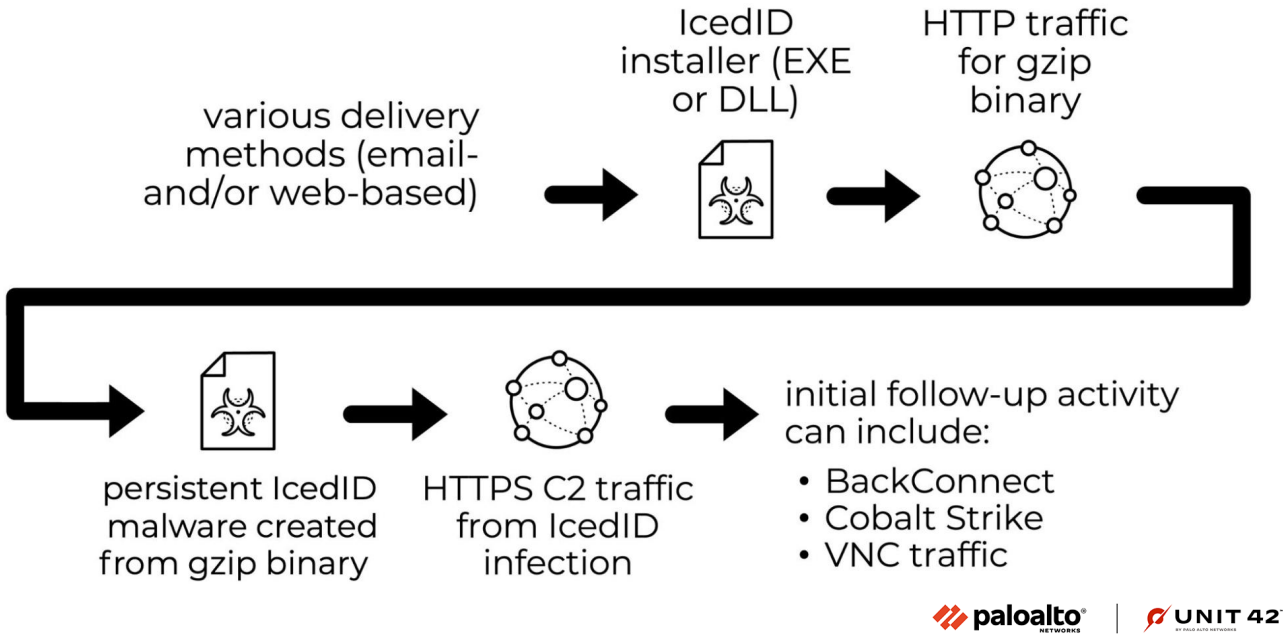

Figure 1. Flowchart for chain of events in the April 2023 IcedID infection.

Most IcedID infections use a standard variant of IcedID. These infections typically use an EXE or DLL that acts as an installer. This installer generates an unencrypted HTTP GET request that retrieves a gzip-compressed binary. The installer then converts this binary into malware used for a persistent IcedID infection.

The newly created, persistent IcedID generates HTTPS traffic to communicate with command and control (C2) servers. The C2 activity can lead to BackConnect traffic, Cobalt Strike and Virtual Network Computing (VNC) activity.

If the infected host is part of a high-value environment, an IcedID infection would likely lead to ransomware.

Pcap Analysis: Infection Vector

Using Wireshark customized from our tutorials, apply a basic web filter to see if anything stands out. Review the results in your column display. Look for unencrypted HTTP traffic over TCP port 80 directly to an IP address without an associated domain. This is a common characteristic in the chain of events for various malware infections.

At 15:31:08 UTC, the host at 10.4.19[.]136 generated an HTTP GET request to hxxp://80.77.25[.]175/main.php as shown below in Figure 2.

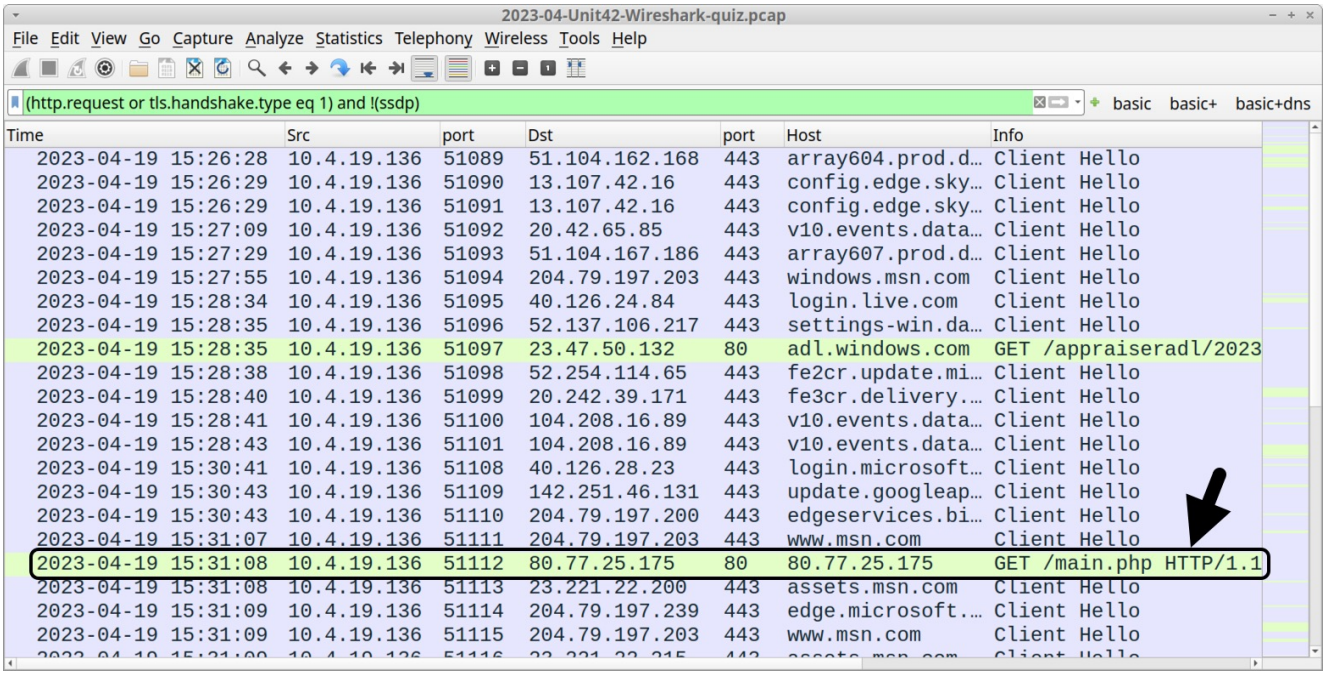

Figure 2. Suspicious HTTP traffic directly to an IP address shown in Wireshark.

Follow the TCP stream for this HTTP GET request, as shown in Figure 3. This should generate a window for TCP stream 32, as shown in Figure 4.

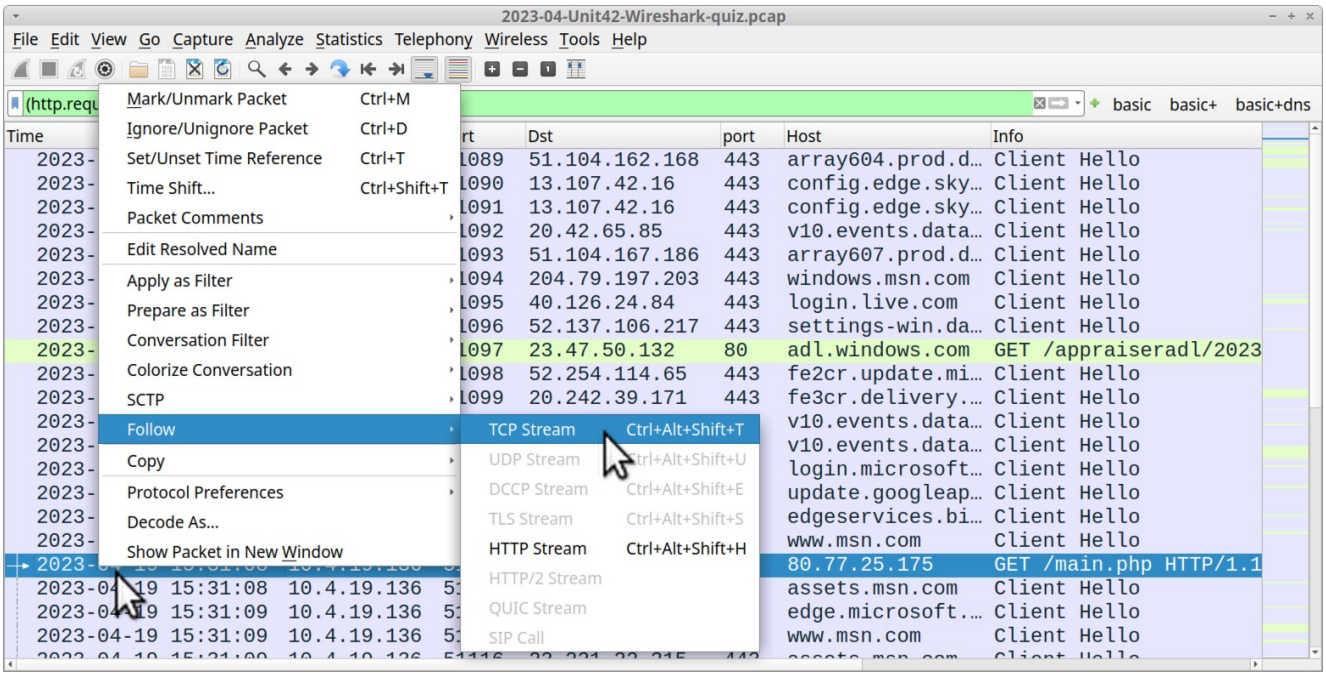

Figure 3. Following TCP stream for suspicious HTTP GET request.

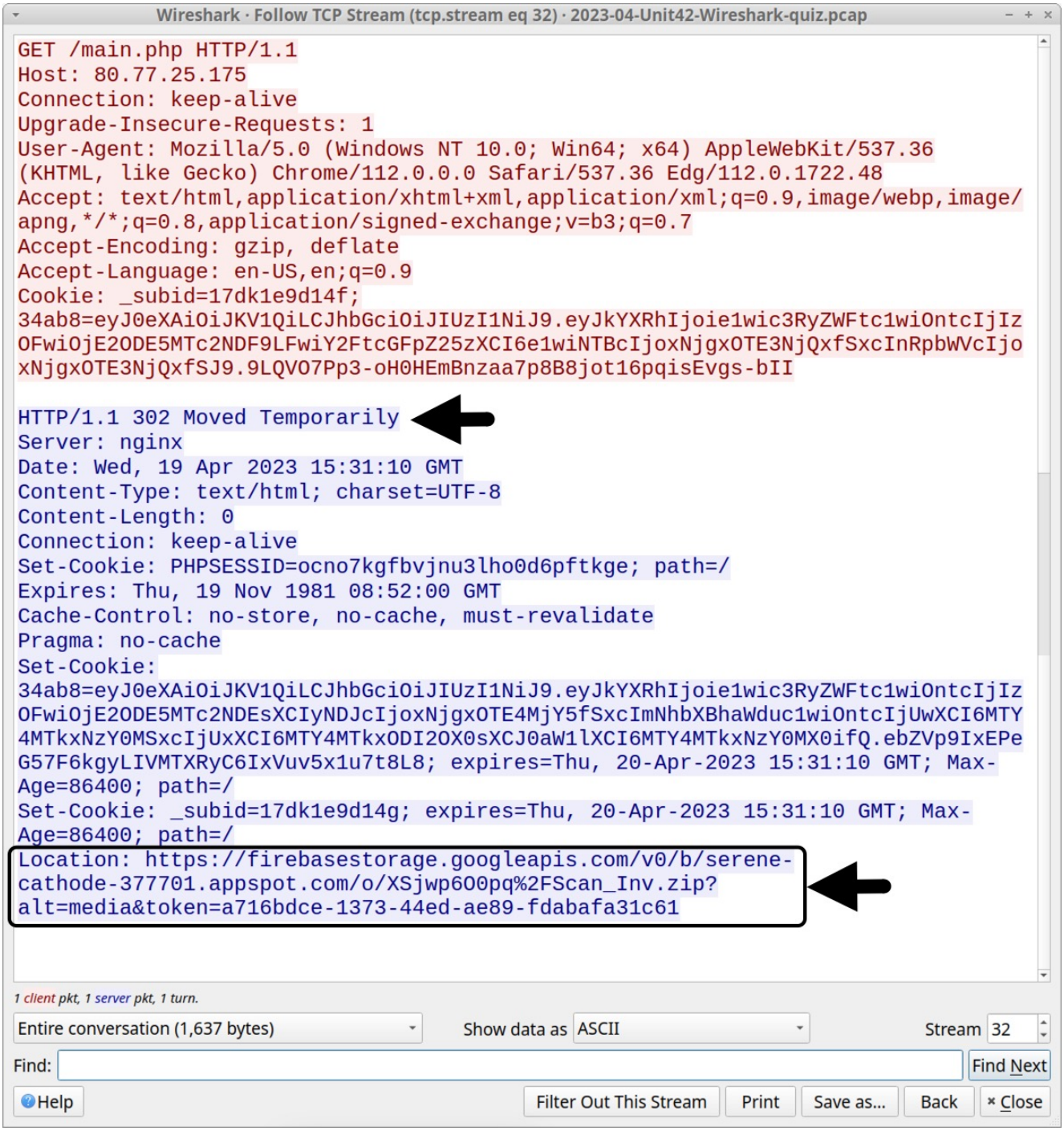

Figure 4. TCP stream for the suspicious HTTP GET request and response.

Figure 4 reveals HTTP request headers that contain a User-Agent string ending with Edg/112.0.1722.48. This string indicates the traffic was likely generated by the Microsoft Edge browser. However, web traffic generated by malware can spoof different User-Agent strings, and some browser extensions also have this ability, so we cannot be certain this was actually Microsoft Edge.

The HTTP response headers in Figure 4 show a 302 code, redirecting traffic to the following URL:

hxxps://firebasestorage.googleapis[.]com/v0/b/serene-cathode-377701.appspot.com/o/XSjwp6O0pq%2FScan_Inv.zip?alt=media&token=a716bdce-1373-44ed-ae89-fdabafa31c61

This Firebase Storage URL has been reported as malicious by at least seven security vendors on VirusTotal, and it appears in URLhaus tagged as IcedID. Fortunately, Google has taken the URL offline, and it is no longer active.

To further refine our search, add the client's IP address 10.4.19[.]136 to the basic web filter as shown below in Figure 5. This reveals HTTPS traffic to firebasestorage.googleapis[.]com shortly after traffic to the initial URL at hxxp://80.77.25[.]175/main.php.

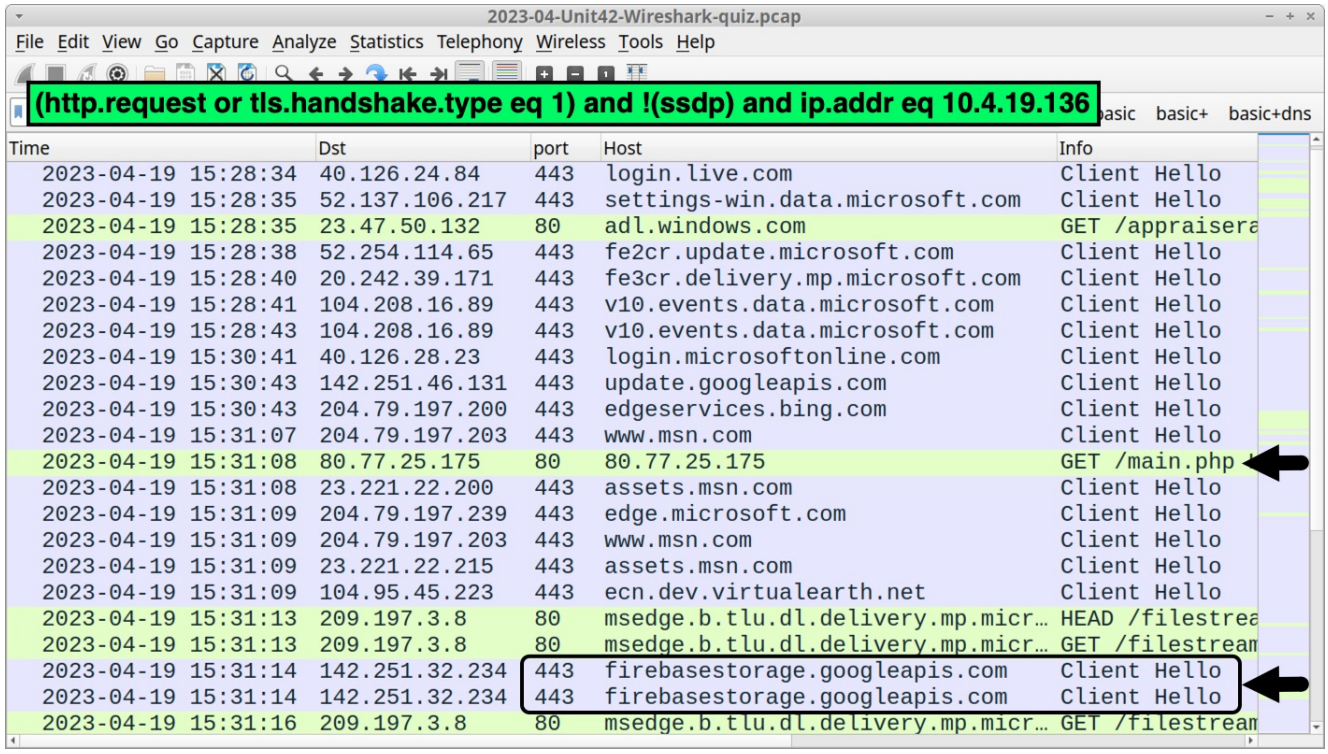

Figure 5. HTTPS traffic to firebasestorage.googleapis[.]com after the initial suspicious URL.Follow the TCP stream for the initial frame showing fire in the Wireshark column display. The TCP stream reveals 273 KB of data sent from the server to the Windows host, as shown below in Figure 6. This indicates a file might have been sent to the Windows host.

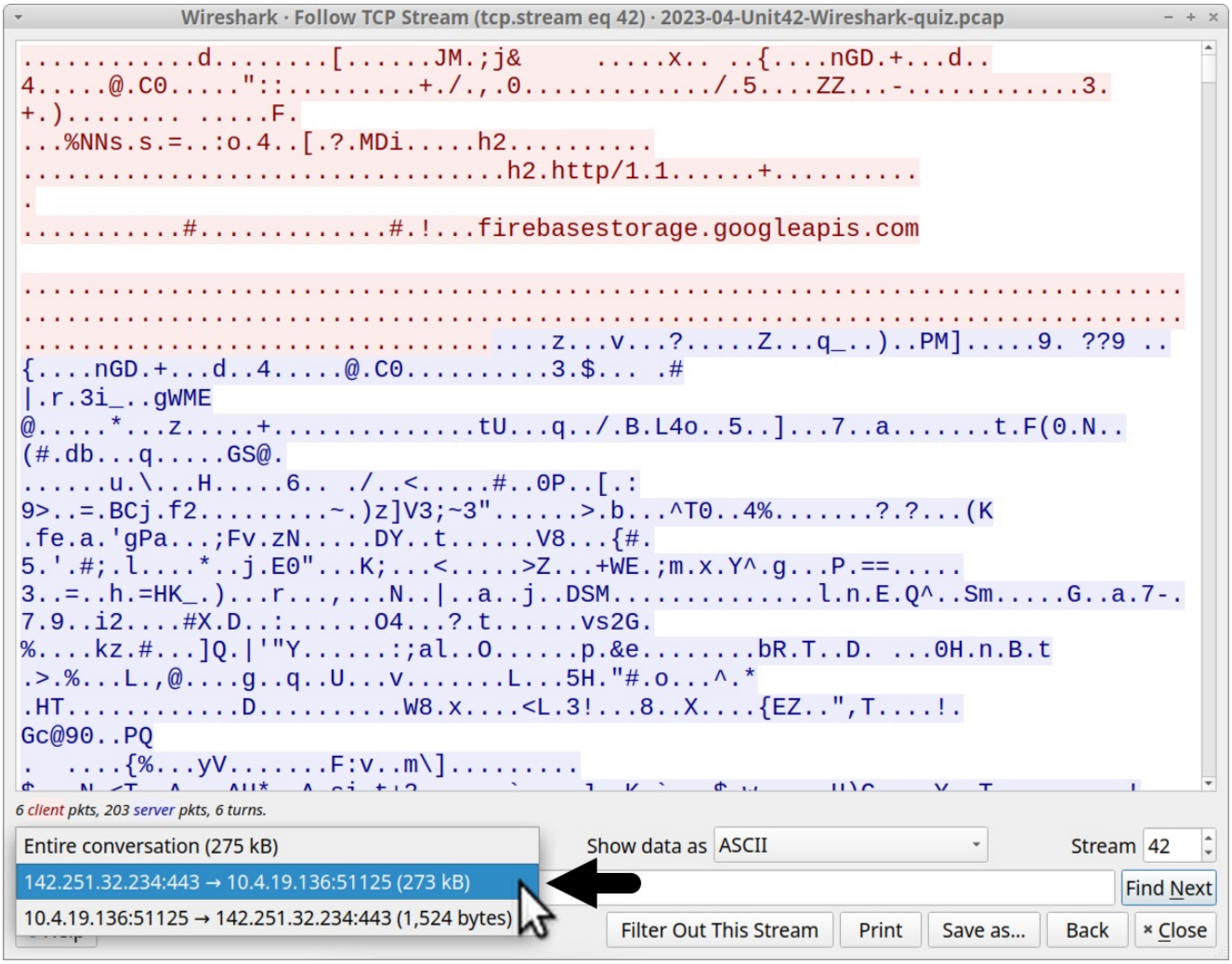

Figure 6. TCP stream showing 275 KB of data sent from firebasestorage.googleapis[.]com to the Windows host.While the Firebase Storage URL is tagged as IcedID on URLhaus, this only indicates a distribution method for the IcedID installer. Based on this pcap, the victim opened a link that led to the Firebase Storage URL, and that URL delivered a file for an IcedID installer. The URLhaus entry for this Firebase Storage URL reveals the ZIP archive it previously hosted, as shown in Figure 7.

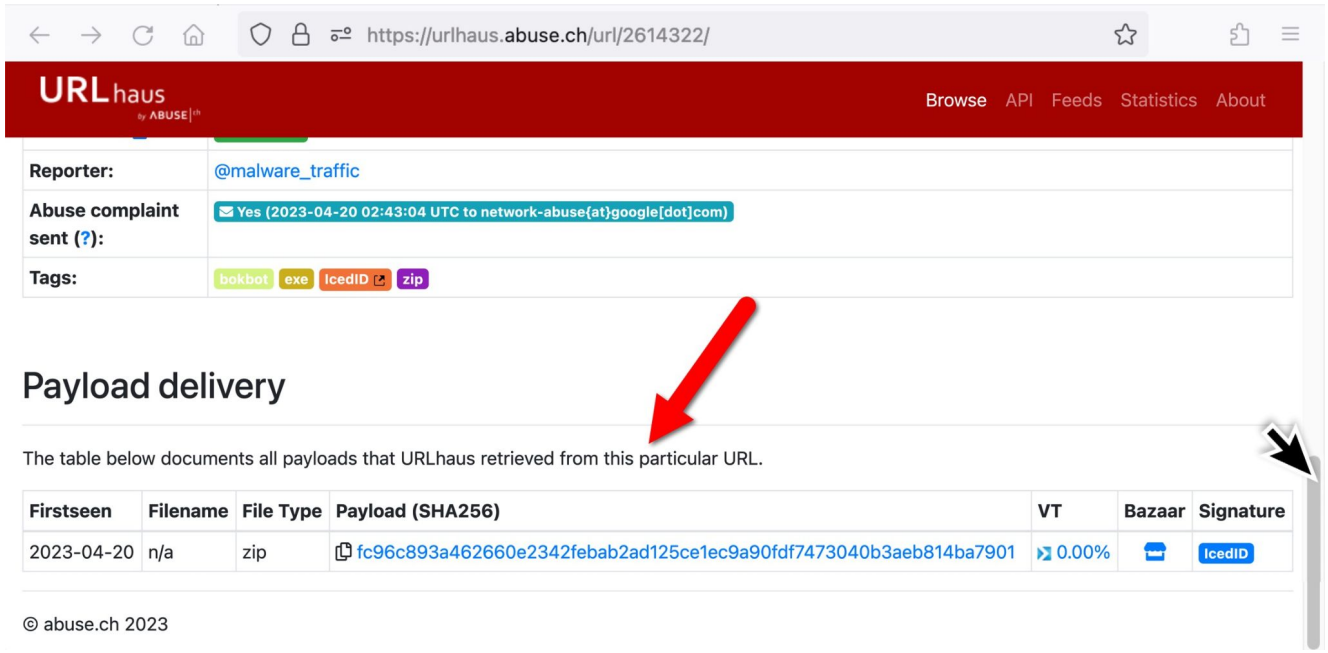

Figure 7. URLhaus entry for our firebasestorage URL shows it delivered a zip archive.

The ZIP archive was submitted to Malware Bazaar. The archive is password-protected with the ASCII string *1235*, and it contains a file named Scan_Inv.exe. This Windows executable file is an IcedID installer.

Pcap Analysis: IcedID Traffic

An IcedID loader first generates an unencrypted HTTP GET request over TCP port 80 to a domain using GET / without any further URL. This returns a gzip binary used by the installer to create the persistent malware on the victim's host.

To find the gzip binary, use the same basic web filter with the victim's IP address noted earlier in Figure 5. Scroll down to an HTTP GET request to skigimeetroc[.]com at 15:35:39 UTC and follow the TCP stream as shown below, in Figure 8.

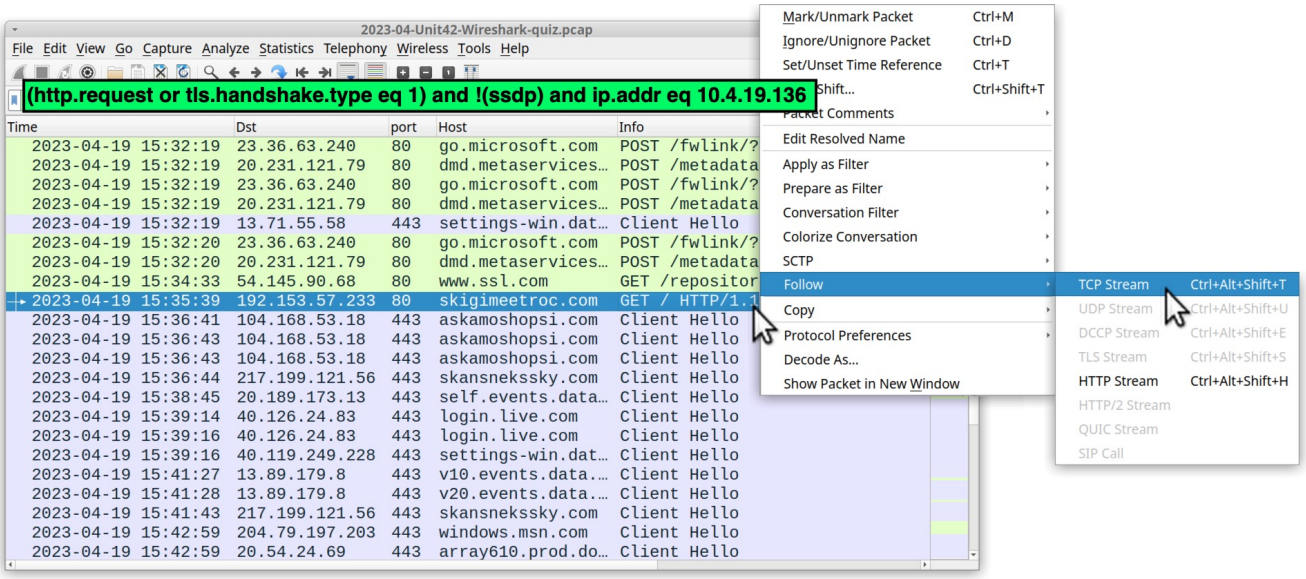

Figure 8. Following the TCP stream for IcedID installer's initial HTTP GET request.

This is TCP stream 53 from the pcap, as shown below in Figure 9. The HTTP request headers for traffic generated by the IcedID installer have no User-Agent string. Note the cookie sent in the request headers in Figure 9.

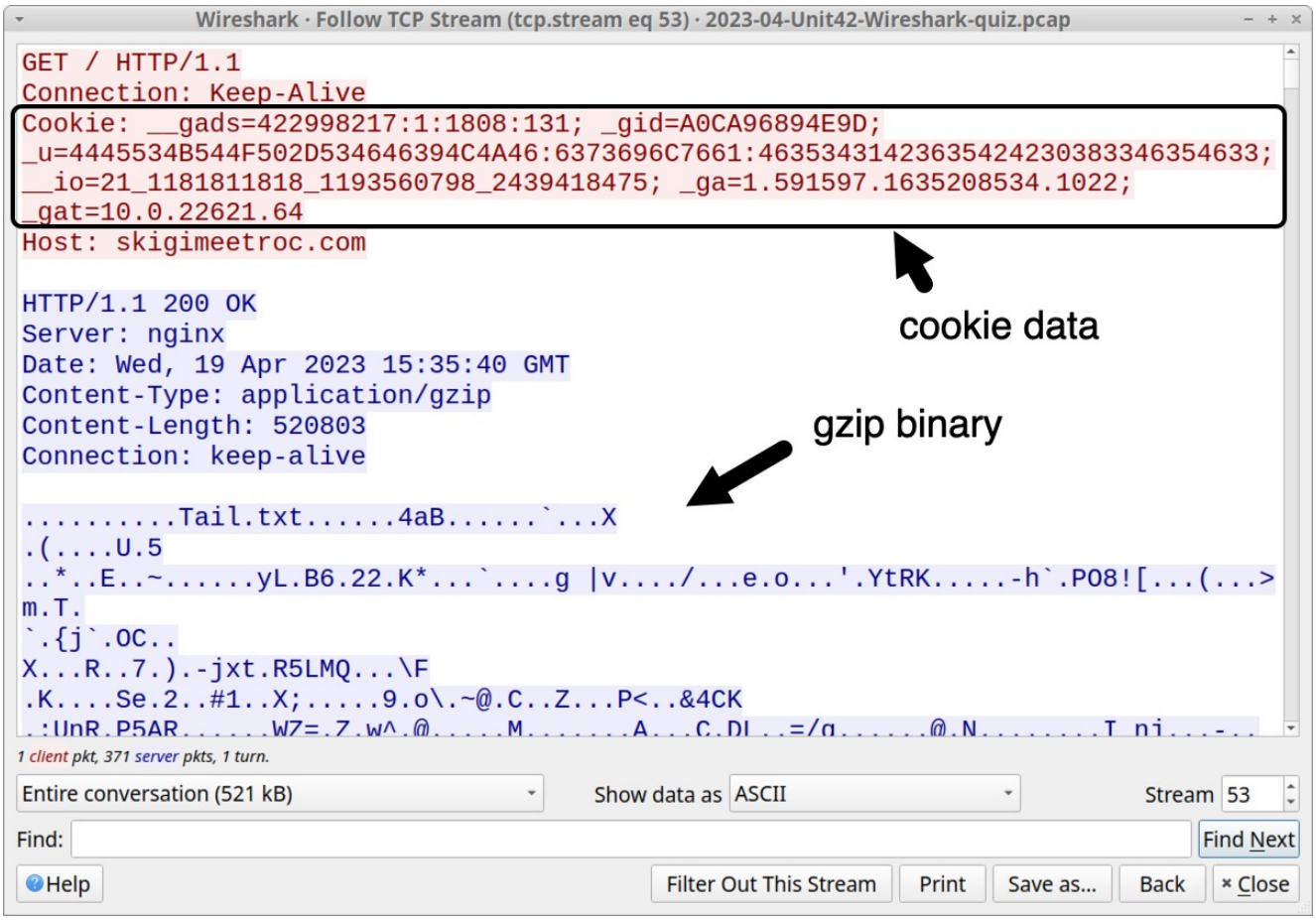

Figure 9. HTTP GET request generated by the IcedID installer.
The cookie line follows:

Cookie: __gads=422998217:1:1808:131; _gid=A0CA96894E9D;
_u=4445534B544F502D534646394C4A46:6373696C7661:463534314236354242303833346354633;
__io=21_1181811818_1193560798_2439418475; _ga=1.591597.1635208534.1022;
_gat=10.0.22621.64

Cookie parameters for the HTTP GET request caused by this IcedID installer follow:

- __gads= IcedID campaign identifier and information from the infected host.
- _gid= Value calculated using MAC address of the infected host.
- _u= ASCII text representing hex values of the victim's hostname, Windows user account name and another undetermined value.
- __io= Domain identifier from the infected host's security identifier (SID).
- _ga= Information based on the infected host's CPU.
- _gat= Windows version. For example, 10.0.22621.64 is an identifier for 64-bit Windows 11 version 22H2 and 10.0.19045.64 is an identifier for 64-bit Windows 10 version 22H2.

These cookie parameters are unique to IcedID infections. You can identify this traffic as IcedID without understanding the values. However, the _u= parameter reveals the victim's hostname and Windows user account name. This information is very useful for our investigation. These hex values translate to a hostname of DESKTOP-SFF9LJF and a Windows user account name of csilva, as shown below in Figure 10.

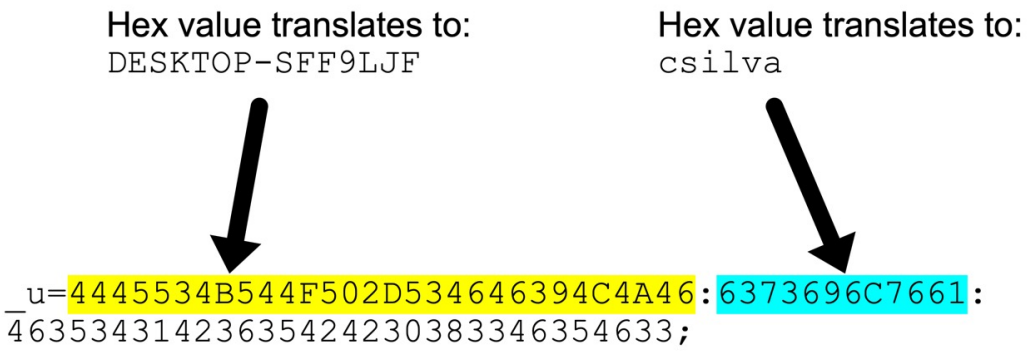

Figure 10.

Using the _u= cookie parameter to determine the victim's hostname and Windows user account name.

After retrieving the gzip binary, an IcedID installer creates persistent IcedID malware that takes over the infection. The infected Windows host then starts generating HTTPS traffic to IcedID C2 servers.

These C2 servers use different domain names and IP addresses than the initial domain contacted by the IcedID installer. IcedID's HTTPS C2 traffic starts within a minute or two after the installer retrieves the gzip binary, and this activity uses at least two domains with random alphabetic names.

Our pcap reveals HTTPS traffic from the infected host to two domains after skigimeetroc[.]com at 15:35:39 UTC. These HTTPS C2 servers are askamoshopsi[.]com on 104.168.53[.]18 and skansnekssky[.]com on 217.199.121[.]56.

To find these servers, use the same basic web filter with the victim's IP address noted earlier in Figure 5. HTTPS traffic starting at 15:36:41 UTC reveals these domains, as shown below in Figure 11.

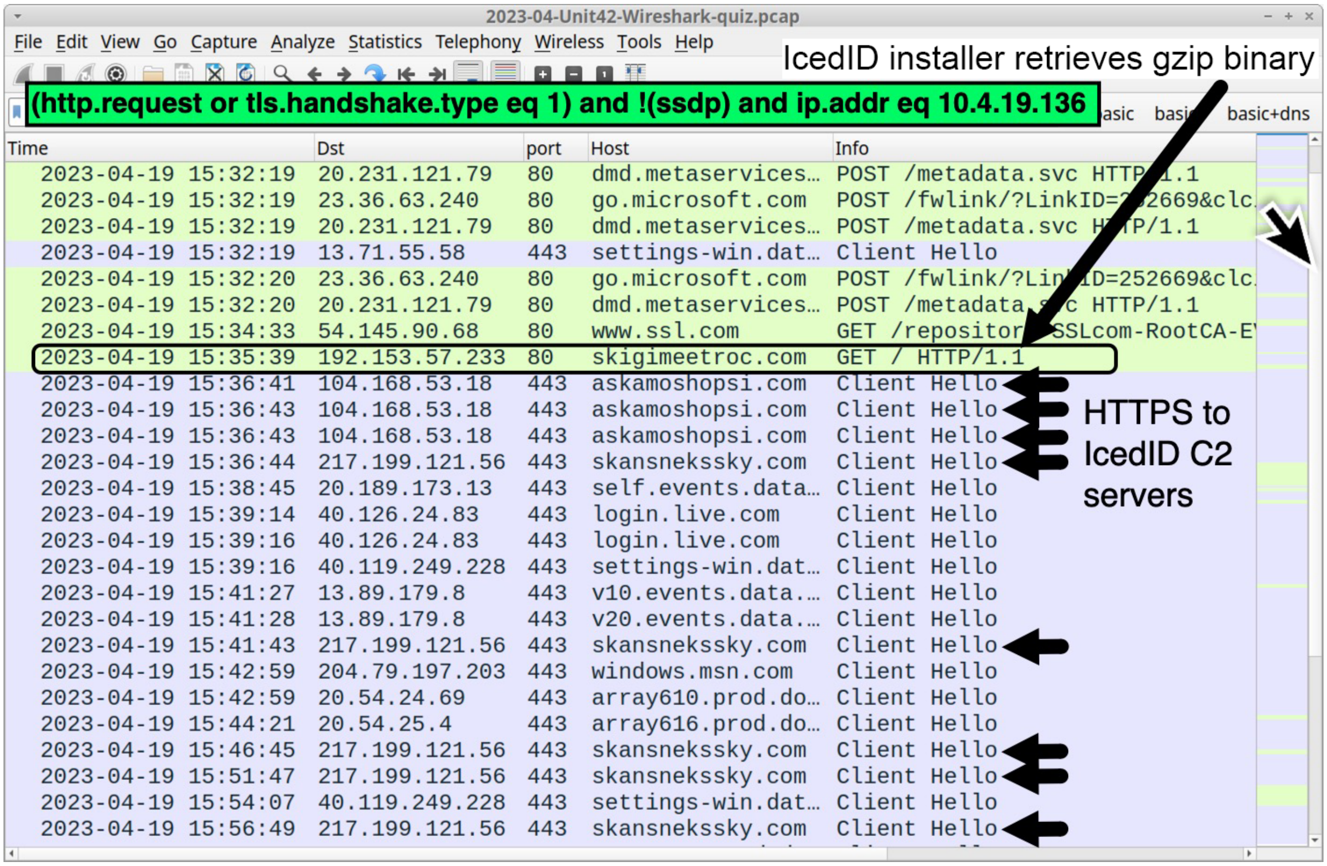

Figure 11. HTTPS C2 traffic after HTTP request by the IcedID installer.

Both C2 servers at askamoshopsi[.]com and skansnekssky[.]com use self-signed certificates for their HTTPS traffic. Self-signed certificates for HTTPS traffic will generate warnings about potential security risks when the site is viewed in any modern web browser.

Why do web browsers display warnings about websites that use self signed certificates? Because these are not validated by a Certificate Authority. Criminals can generate self-signed certificates that impersonate an existing company, or they can use generic values for the certificate issuer. Without a validated certificate, web browsers cannot be sure a website is what it says it is.

Figure 12 shows what the server at askamoshopsi[.]com looked like when we attempted to view it with the Firefox web browser. This warning allows users to view the server's self-signed certificate.

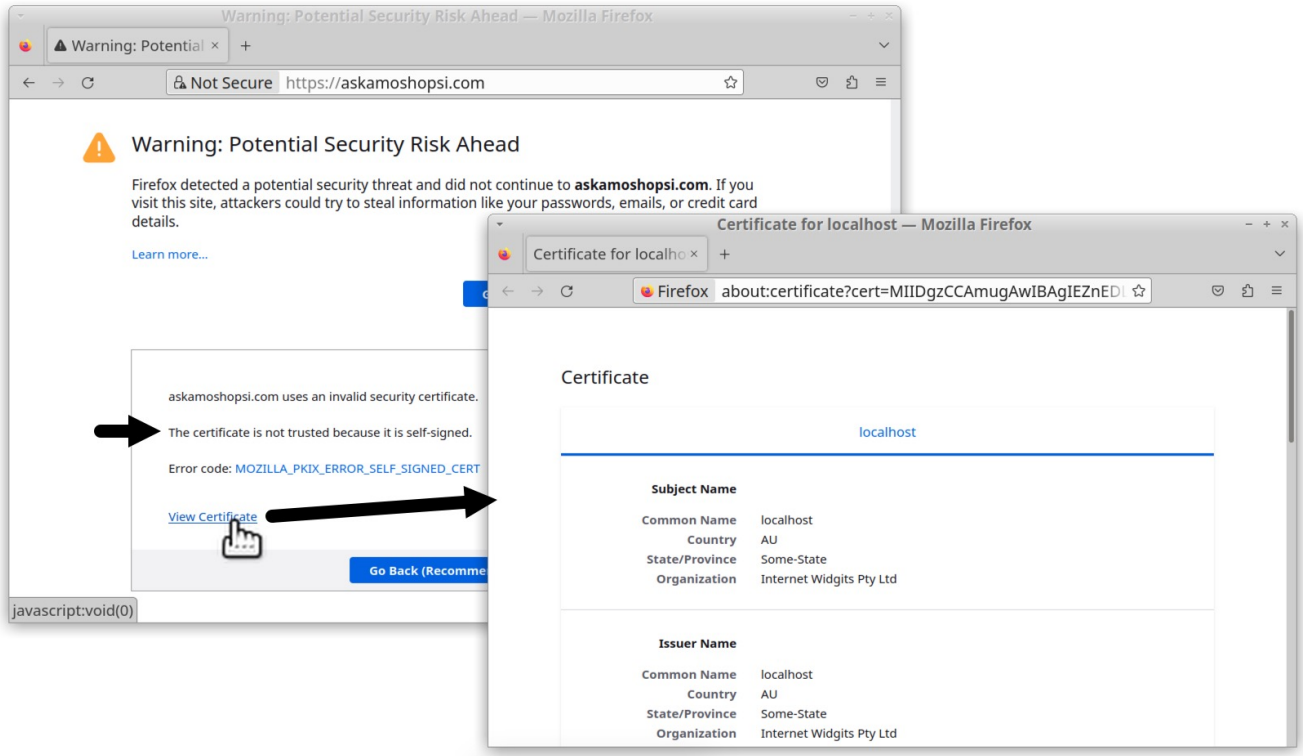

Figure 12. Attempting to view the web server at askamoshopsi[.]com using Firefox.As shown above in Figure 12, the certificate uses values like Internet Widgits Pty Ltd for the issuer's Organization name and Some-State for the State/Province name. Values for self-signed certificates used by IcedID C2 servers are the same default values seen when using OpenSSL to create a certificate in Xubuntu as shown below in Figures 13 and 14.

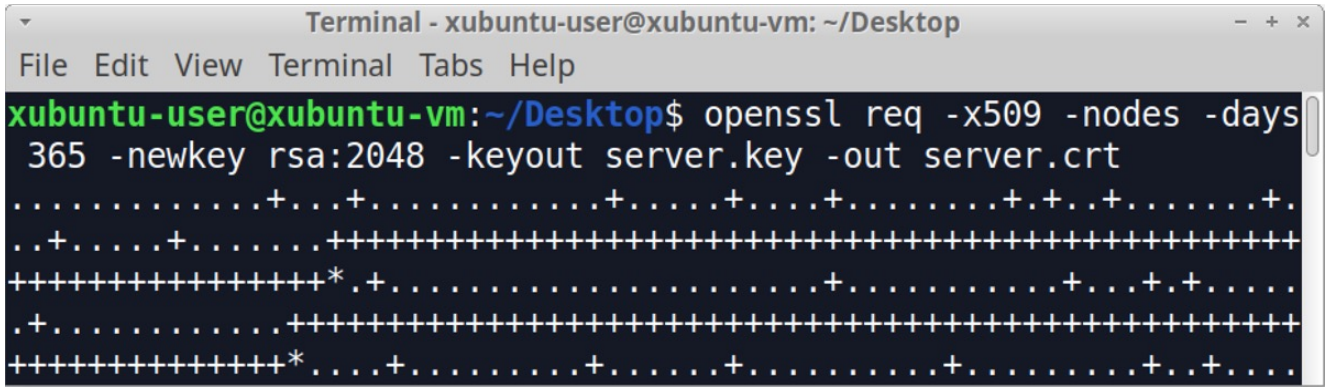

Figure 13. Creating an x509 certificate for a web server using OpenSSL in Xubuntu.

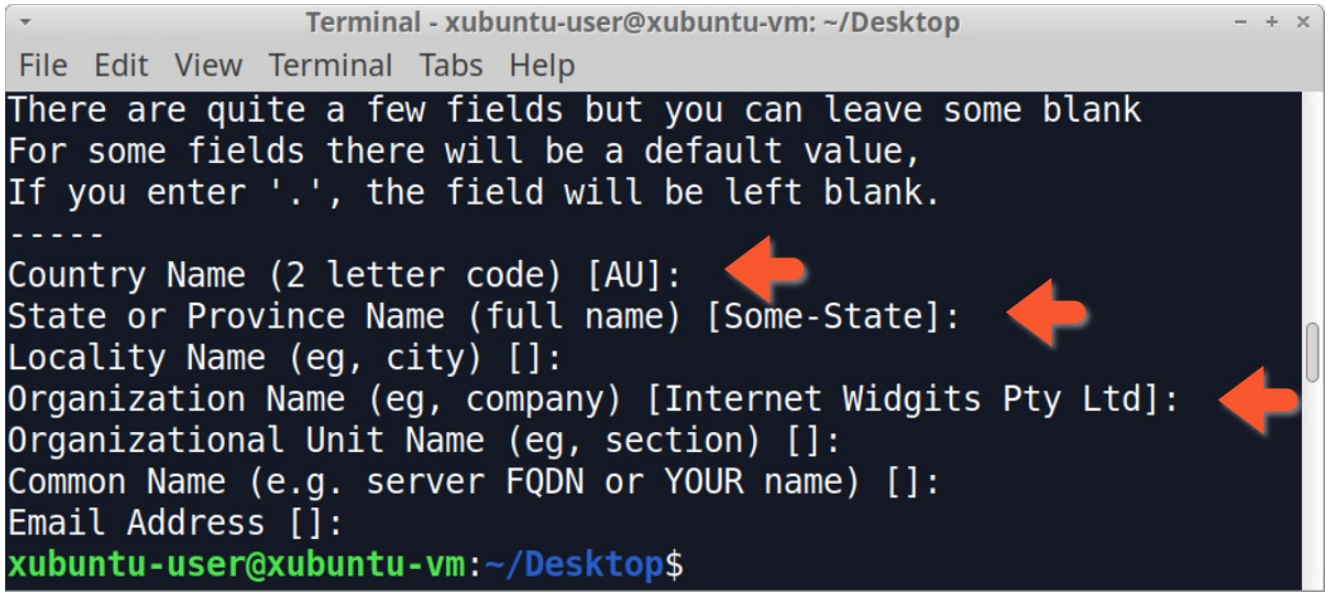

Figure 14. Default values when creating an x509 certificate for a web server using OpenSSL in Xubuntu.

Since Internet Widgits Pty Ltd is a default value for a self-signed certificate in HTTPS traffic, and this value is sometimes seen in C2 traffic for malware. This should be more closely examined if it's found when investigating a suspected malware infection. We can easily check any pcap for this value using the following Wireshark filter:

x509sat.uTF8String eq "Internet Widgits Pty Ltd"

The results from our pcap reveal the same IP addresses used by IcedID C2 servers for askamoshopsi[.]com at 104.168.53[.]18 and skansnekssky[.]com at 217.199.121[.]56. Expand the frame details for any of the results to find the same certificate issuer data, as shown in Figure 15.

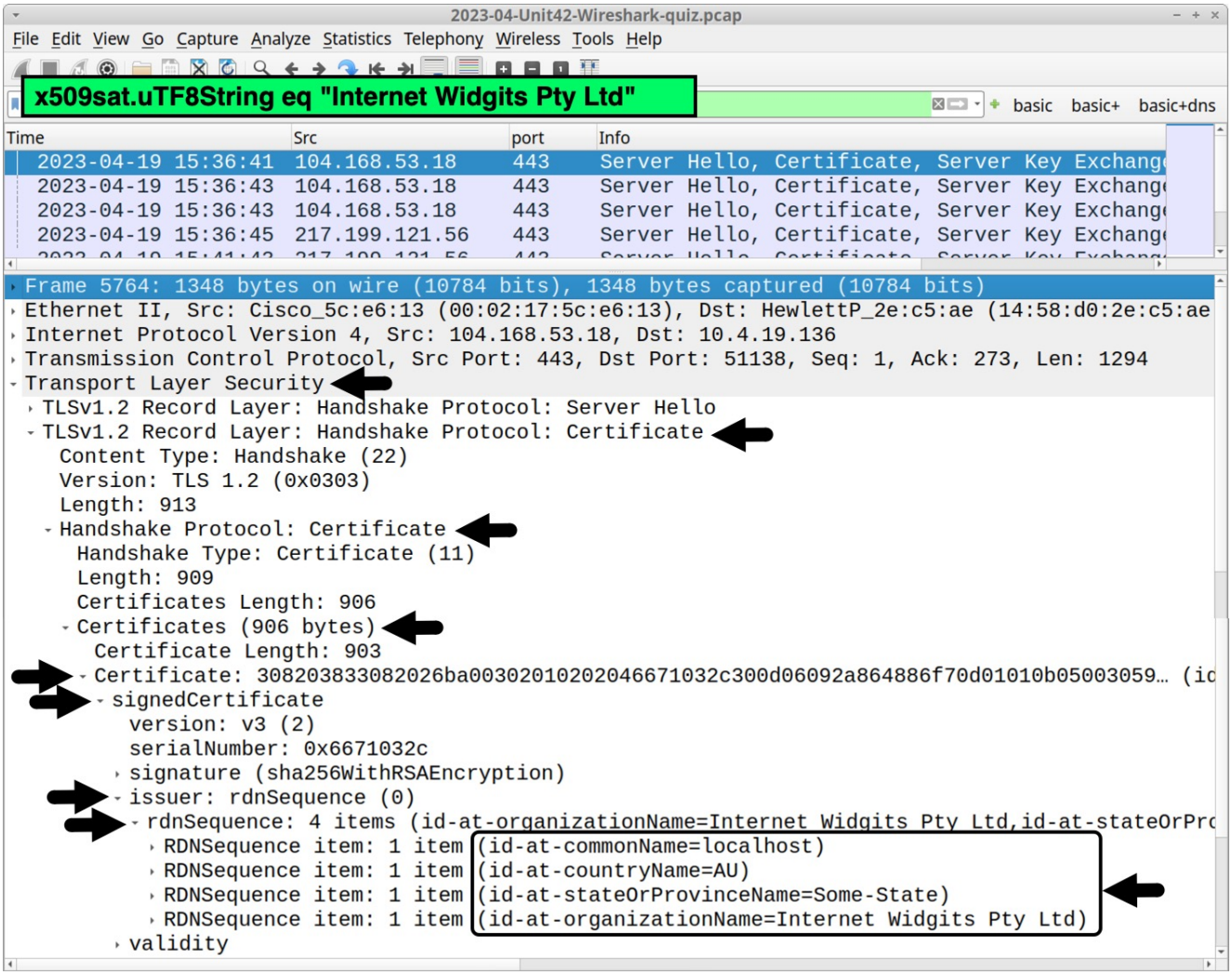

Figure 15. Self-signed certificate by IcedID C2 servers using Internet Widgits Pty Ltd as the Organization name shown in Wireshark.

This certificate data is not unique to IcedID. The same values for self-signed certificates are also seen in HTTPS C2 traffic by other malware families like Bumblebee.

Pcap Analysis: BackConnect Traffic

Undetected IcedID infections lead to follow-up activity like BackConnect traffic.

For the past several months, BackConnect traffic caused by IcedID was easy to detect because it occurred over TCP port 8080. However, as early as April 11, 2023, BackConnect activity for IcedID changed to TCP port 443, making it harder to find.

This BackConnect activity from IcedID Unit 42 tweeted on April 11, 2023 used an IP address of 193.149.176[.]100 over TCP port 443. Filter for that IP address in Wireshark and combine it with tcp.flags eq 0x0002 as shown below, in Figure 16. This reveals the beginning of three streams.

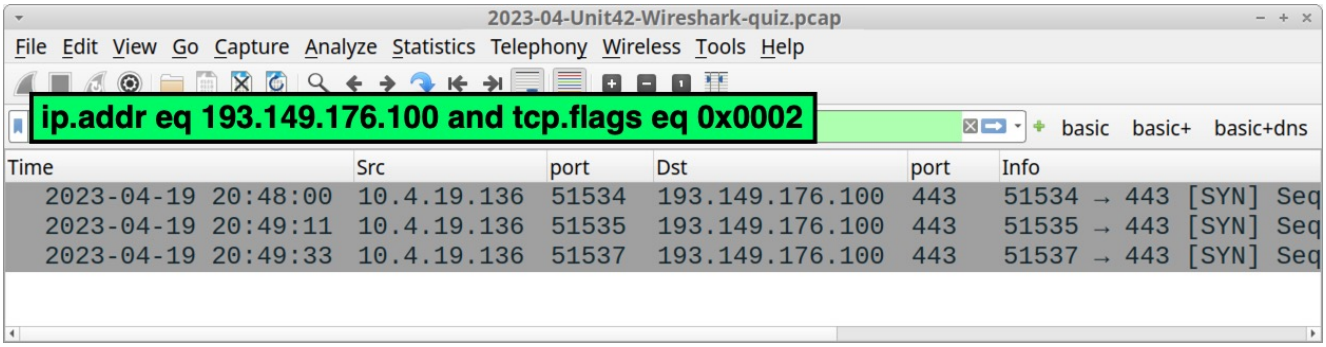

Figure 16. Filtering in Wireshark for BackConnect traffic in our pcap.

Follow the TCP stream for the first result, which is TCP stream 950. This stream reveals encoded or otherwise encrypted TCP traffic, as shown in Figure 17.

Figure 17. The first TCP stream for BackConnect activity.

Go back to the Wireshark filter used to reveal the TCP streams to 193.149.176[.]100. Follow the TCP stream for the second frame in the results, which is TCP stream 951. This reveals encoded or encrypted data followed by a command to reveal all hosts under the domain controller for boogienights[.]live as shown below, in Figure 18.

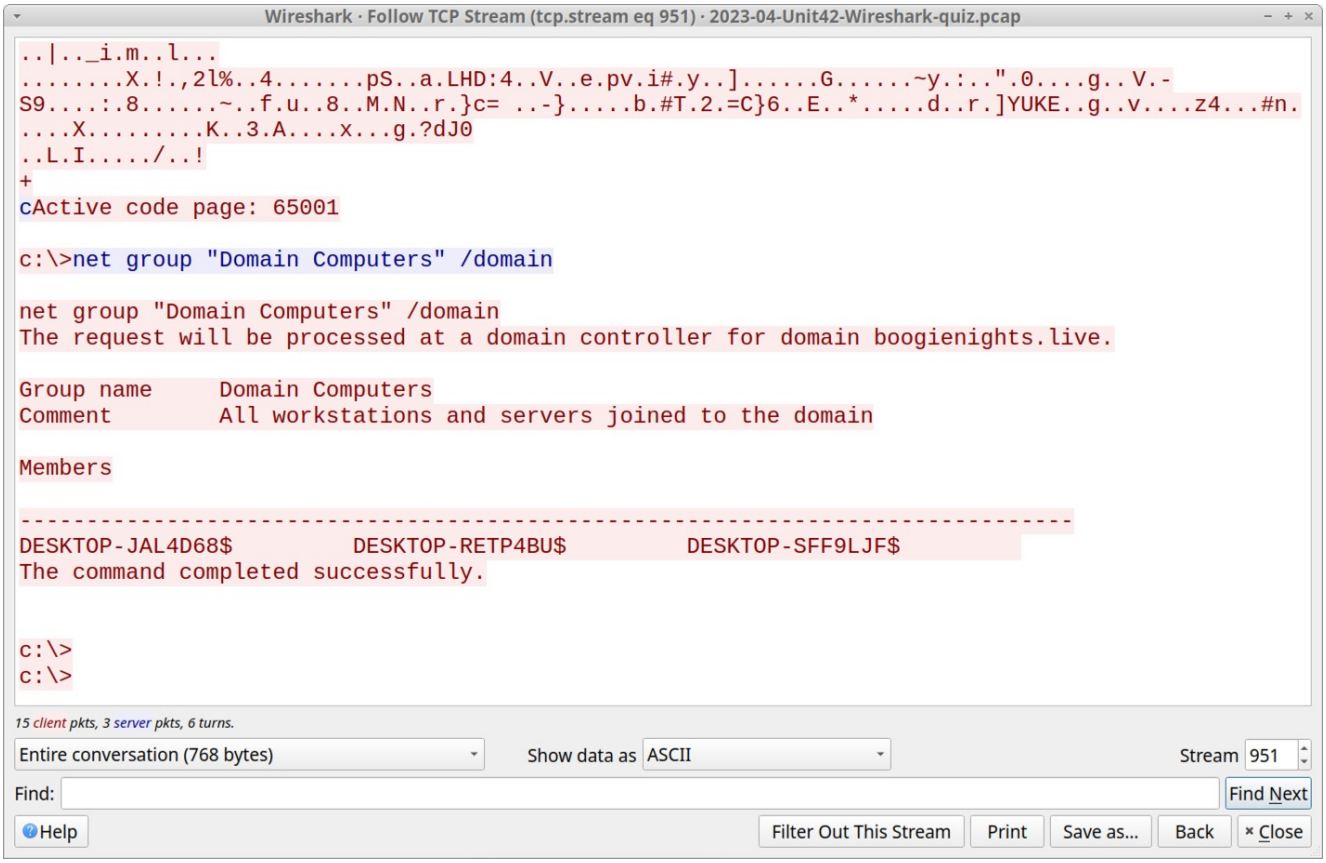

Figure 18. BackConnect traffic with a command to and results enumerating the victim's AD environment.

The response to this command enumerates the victim's AD environment, showing three clients logged in to the domain:

- DESKTOP-JAL4D68
- DESKTOP-RETP4BU
- DESKTOP-SFF9LJF

Go back to the Wireshark filter used to reveal the TCP streams to 193.149.176[.]100. Follow the TCP stream for the last frame in the results, which is TCP stream 953. This lists disk drives on the victim client, and it provides a directory listing for each of these drives, as shown below in Figure 19.

The C:\ drive is the victim's system drive. Z:\ is likely a mapped drive from a server's shared directory that does not contain any files.

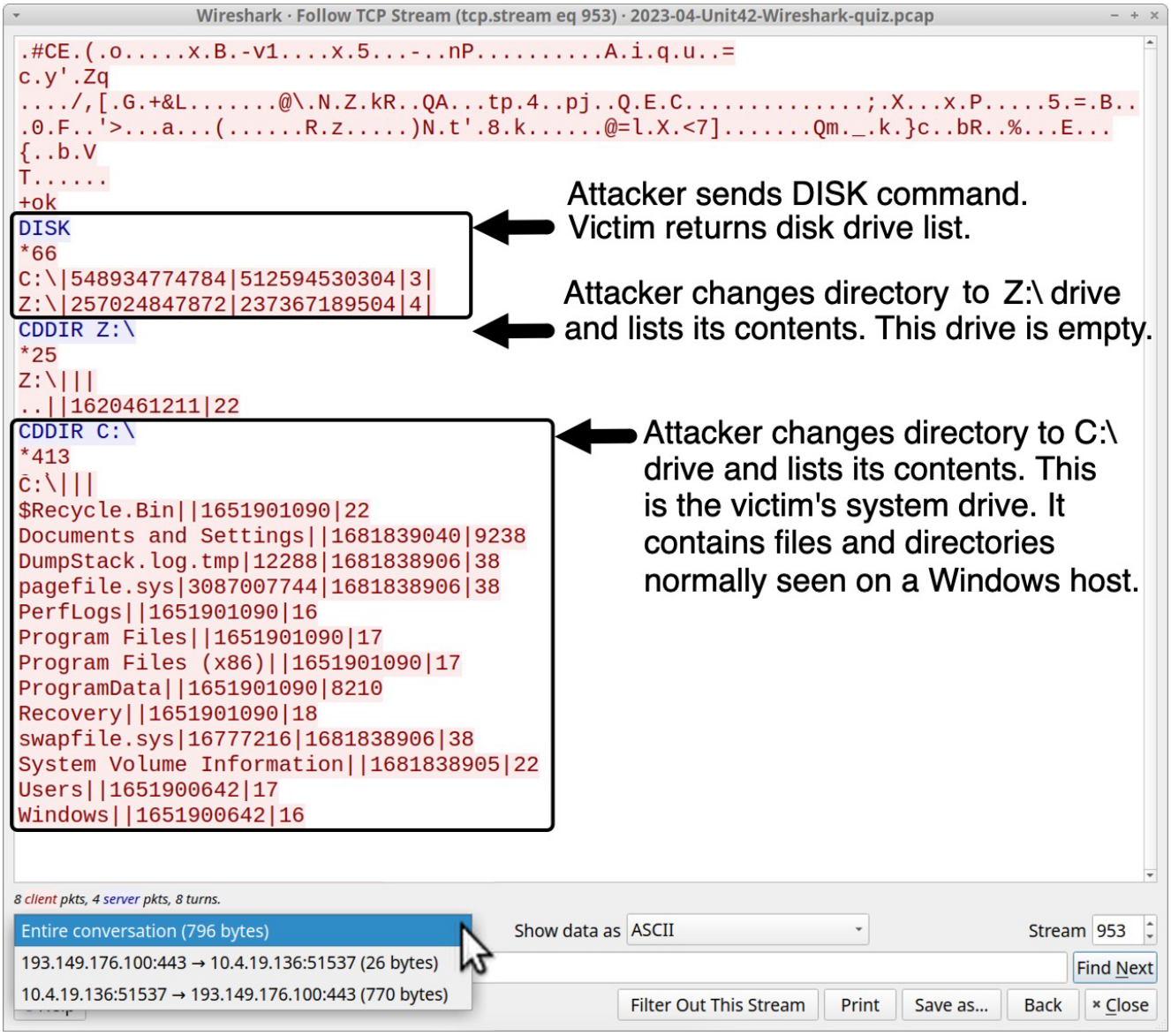

Figure 19. BackConnect traffic showing contents of the victim's system drive and mapped drive.

Previous IcedID infections reveal this threat can use BackConnect traffic to load and run Cobalt Strike. We tweeted about one such case from March 24, 2023. However, this pcap does not contain any indicators of Cobalt Strike.

Previous IcedID infections also reveal this threat can generate VNC traffic over the same IP address used by BackConnect traffic. This happened during the same IcedID infection from March 24, 2023.

Pcap Analysis: Victim Details

The common internal IP address for the malicious traffic we have reviewed is 10.4.19[.]136. This is our victim's IP address. To find the Windows user account name, filter on that IP address and kerberos.CNameString as shown in Figure 20.

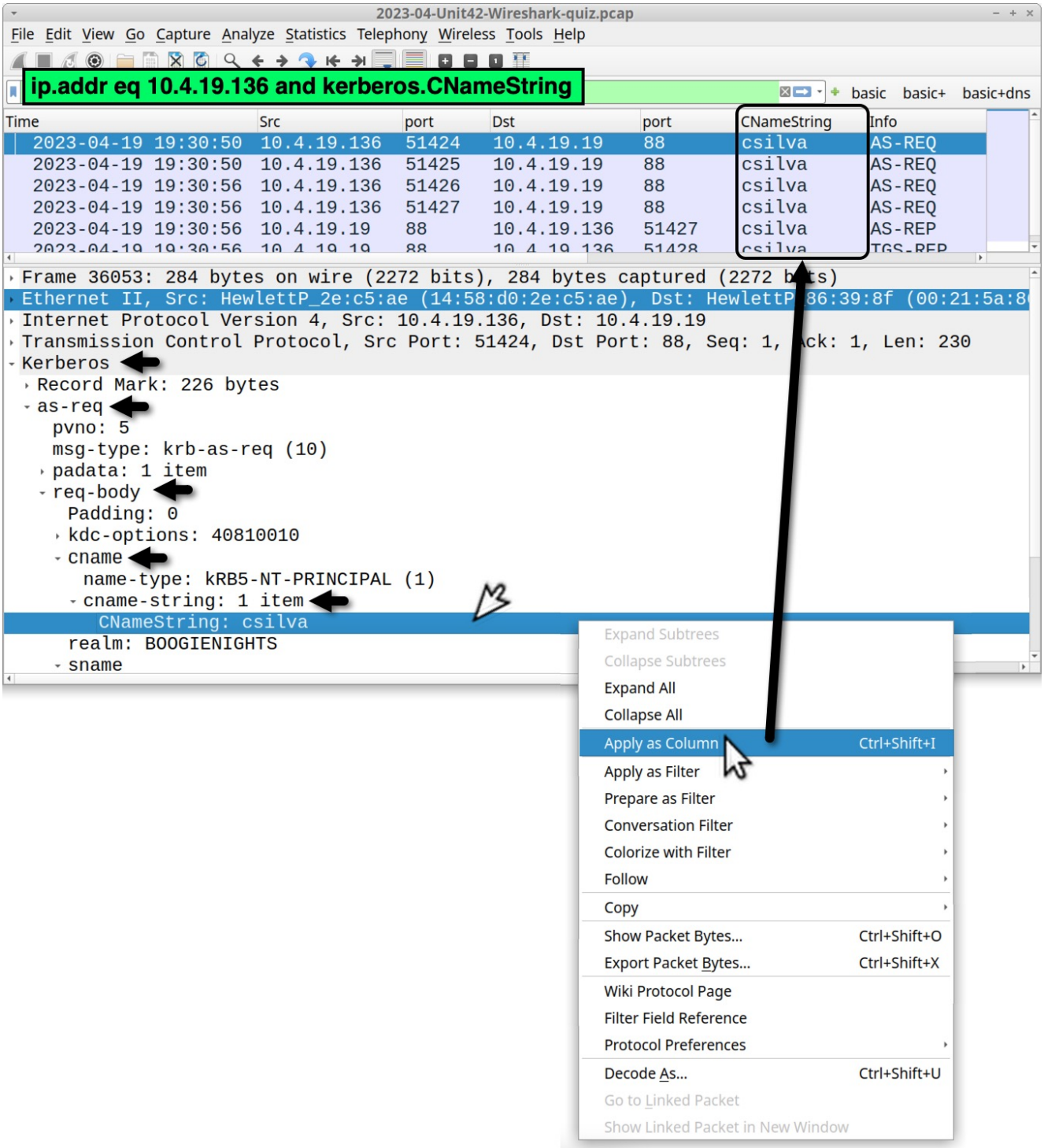

Figure 20. Finding the Windows user account name for our infected Windows host.

In some cases, lightweight directory access protocol (LDAP) might also provide the full name of the user. Use the following Wireshark filter:

ldap.AttributeDescription == "givenName"

This should provide four frames in our column display. Select any of them and expand the frame details until you find the user's full name, Cornelius Silva, as shown below in Figure 21.

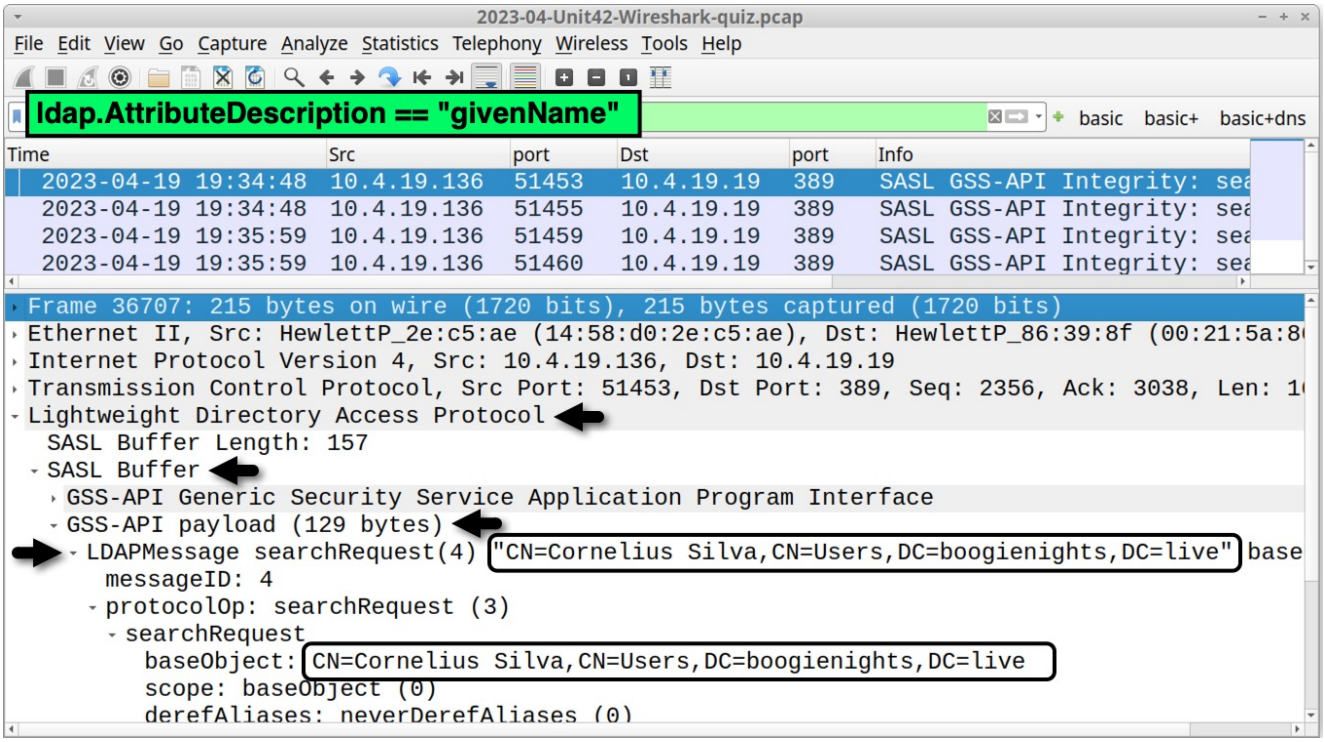

Figure 21. Finding the victim's full name from LDAP traffic.

Perhaps the easiest way to find a victim's hostname in Wireshark is to combine the victim's IP address with a search for ip contains "DESKTOP-" as shown below, in Figure 22. Several results in the info column show Host Announcement DESKTOP-SFF9LJF sent by our infected Windows host at 10.4.19[.]136.

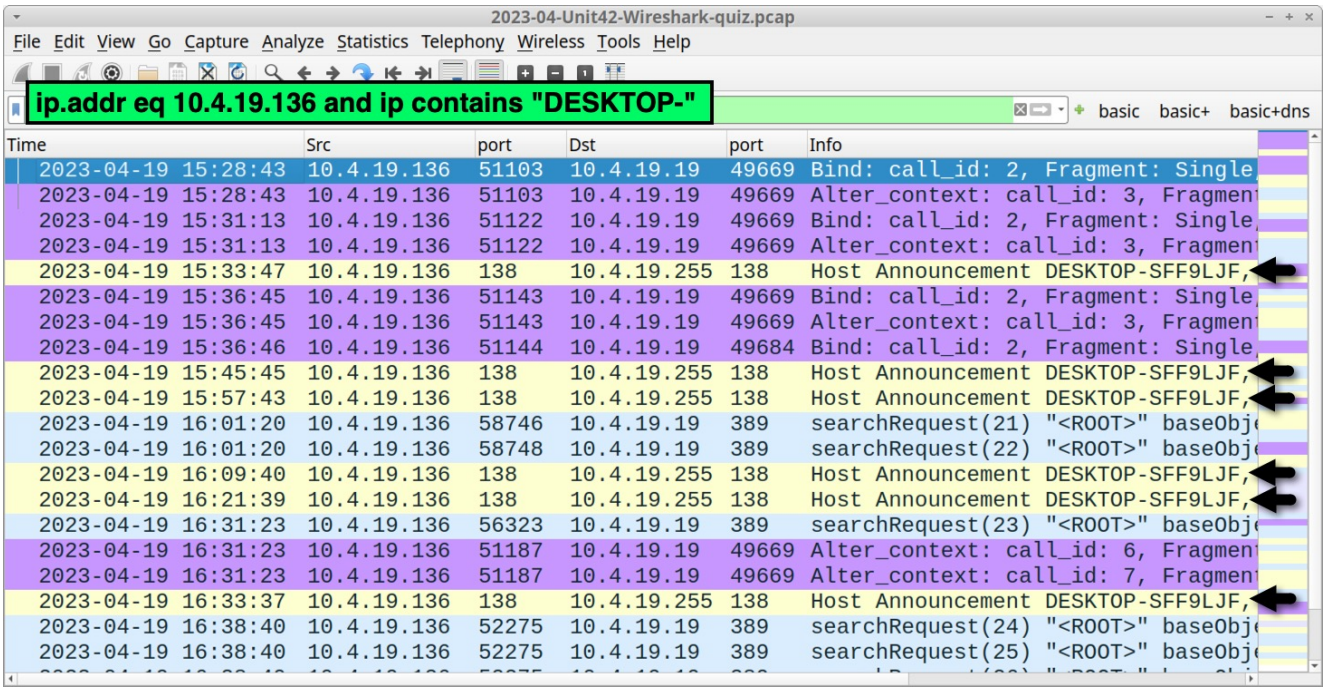

Figure 22. Finding the Windows hostname in Wireshark.

To find the victim's MAC address, just correlate the IP address to the host's MAC address in any of the frame details windows, as shown below in Figure 23.

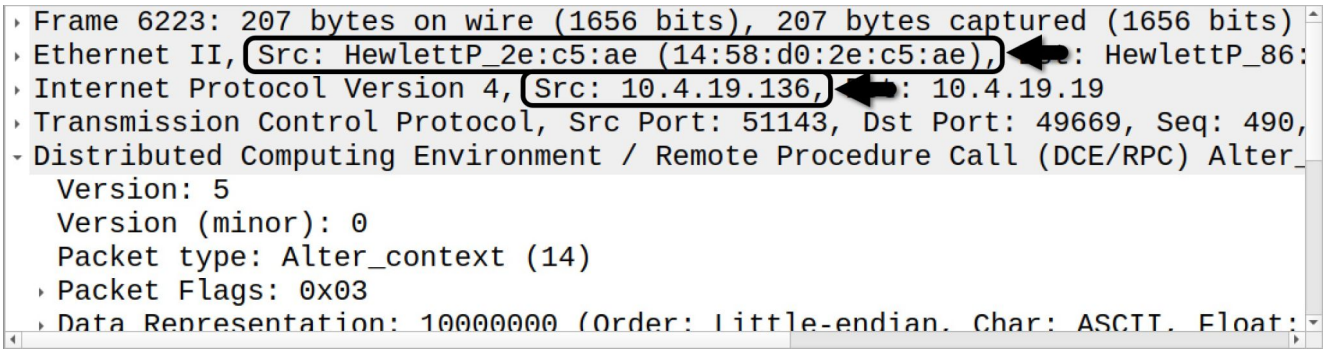

Figure 23. Correlating the victim's MAC address with its associate IP address.

Conclusion

This blog provides answers and analysis for our Unit 42 Wireshark quiz featuring an IcedID infection from April 2023. IcedID is important to identify and stop, because it is a known vector for ransomware infections.

Many organizations lack access to full packet capture in their IT environment. As a result, security professionals might lack experience reviewing IcedID and other malware traffic. Training material like this Wireshark quiz can help. Pcap analysis is a useful skill that helps us better understand malicious activity.

You can also read the original post, without answers, from our standalone quiz post.

Palo Alto Networks customers are protected from IcedID and other malware through Cortex XDR and our Next-Generation Firewall with Cloud-Delivered Security Services that include WildFire, Advanced Threat Prevention and Advanced URL Filtering.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Traffic from the pcap related to the IcedID infection:

- hxxp://80.77.24[.]175/main.php

- hxxps://firebasestorage.googleapis[.]com/v0/b/serene-cathode-377701.appspot.com/o/XSjwp6O0pq%2FScan_Inv.zip?alt=media&token=a716bdce-1373-44ed-ae89-fdabafa31c61
- 192.153.57[.]223:80 - hxxp://skigimeetroc[.]com/
- 104.168.53[.]18:443 - askamoshopsi[.]com - HTTPS traffic
- 217.199.121[.]56:443 - skansnekssky[.]com - HTTPS traffic
- 193.149.176[.]100:443 - BackConnect traffic

Files associated with traffic from this IcedID infection:

Additional Resources

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.