The University of Texas at San Antonio™

ISCS 3523-003 Intrusion Detection and Incident Response

Lab #01 Event Analysis
The SimSpace Cyber Range

Student:
Dillen Dela Cruz, odv464

Prepared for Intrusion Detection and Incident Response
02/03/2024
Professor: Shawn Zumwalt

Contents

Introduction:

Welcome to the network analysis lab, where I will dive into the world of SimSpace Hunt VMs to investigate potential anomalies on a network. In this hands-on session, I will be using Wireshark and Network Miner to examine an ICMP (Internet Control Message Protocol) stream that the user believes might indicate a "significant event" on their home network.

Background:

The user suspects that their home network has experienced a significant event, even though they only use the network for internet access, primarily to connect with their Internet Service Provider (ISP) for email. The nature of this event is unknown, and the user is uncertain about whether it poses any security concerns. Fortunately, they were running Wireshark during the occurrence, capturing the relevant network traffic for further analysis.

Objective:

My objective is to examine the Packet Capture (PCAP) file, conveniently located in a shared folder accessible on Win-Hunt VMs. I will use the capabilities of the tools above to analyze the stream and uncover any potential indicators of compromise or suspicious activities.

Tools for this lab:

Wireshark is a network packet capture tool designed to dissect network packets through filtering and inspection, which can facilitate both real-time and offline analysis. It is a free open-source tool capable of running on practically all operating systems. In 1998, Gerald Combs developed Wireshark with the initial purpose of being able to analyze and optimize traffic generated by the numerous tenants of the small ISP where he was employed (Breeden). Wireshark can capture traffic from various network media types, such as Ethernet, Wireless LAN, Bluetooth, USB, and others. Its graphical user interface (GUI) makes it exceptionally user-friendly and easily customizable, catering to individuals with different backgrounds and experience levels.

Figure 1: Wireshark

Here are some reasons people use Wireshark (Wireshark) :

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

NetworkMiner is a free open-source network forensics tool designed to extract different artifacts, including files, images, emails, and passwords, from captured network traffic within PCAP files (Netresec). Primarily designed for Windows, but available to be used in Linux, can be effectively employed for real-time analysis of network traffic. In February 2017, Erik Hjelmvik created NetworkMiner out of disappointment with the available tools for visualizing devices on the network using PCAP files. Developed during his spare time, NetworkMiner has since evolved into a popular tool for incident response teams and has gained widespread adoption by companies worldwide.

Figure 2: NetworkMiner

Network Mapping:

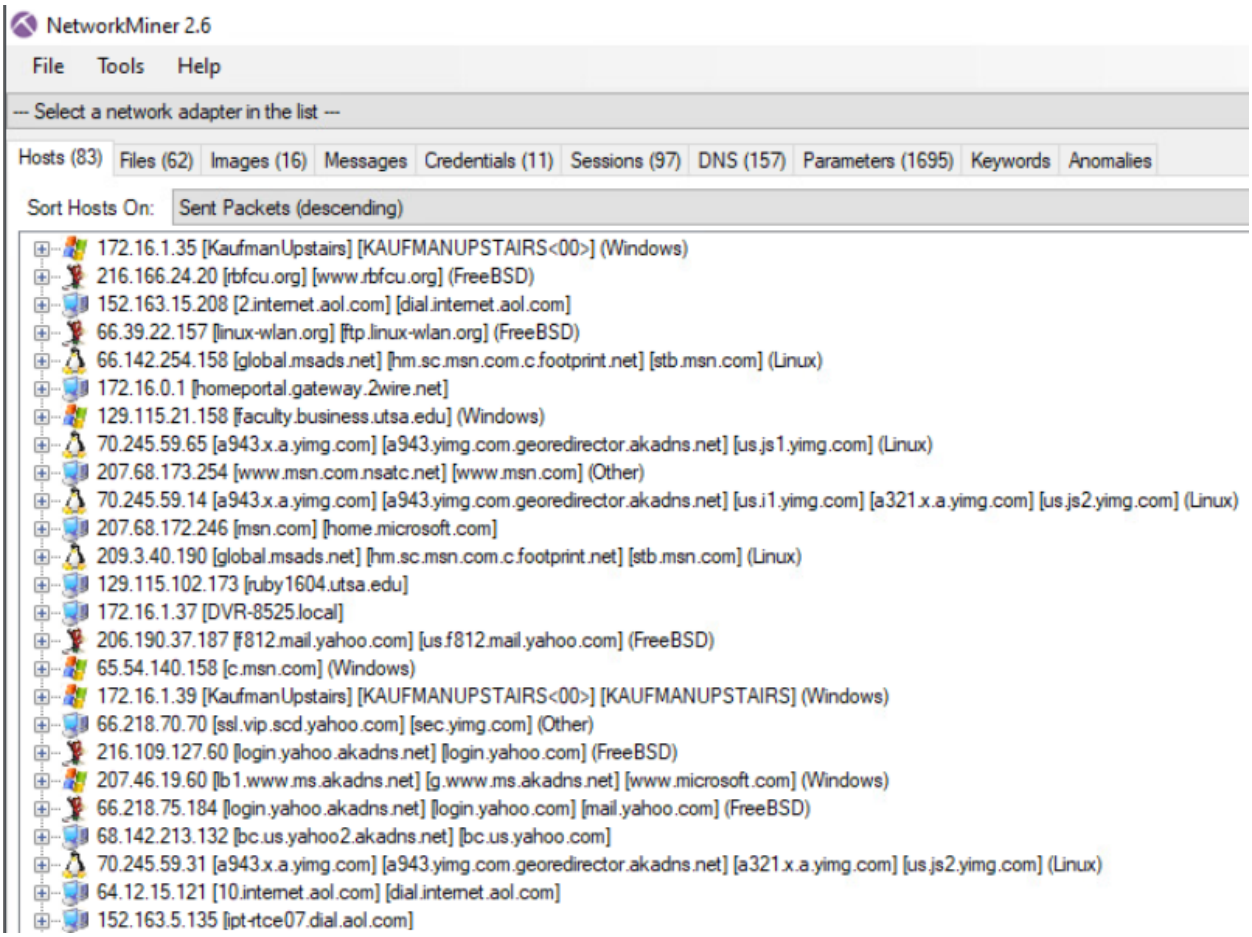


Figure 3: Hosts

Windows OS:

172.16.1.35 – This IP belongs to our client Mr.Kaufman

129.115.21.158 – This IP address is associated with the hostname ‘faculty.business.utsa.edu’. This could be a UTSA specific web server that could contain information on the business department and its faculty. The reason behind this is that investigating the packets further you can see a faculty search on Mr.Kaufman which, if you type in the link, gives you information pertaining to Mr. Kaufman, including details about his department at UTSA, the courses he teaches, contact information, office location, email, and more.

65.54.140.158 – This IP belongs to a specific subdomain of the Microsoft Network web server (c.msn.com). The reason I suspect this is that the ‘referrer’ information within the packet shows that the request originated from 'http://www.msn.com/'.

172.16.1.39 – The IP address 172.16.1.39 is linked to the hostname "Kaufman Upstairs, KAUFMANUPSTAIRS<00>, KAUFMANUPSTAIRS." The occurrence of this similar hostname associated with another IP address (172.16.1.35) raises concerns. It especially intensifies as anomalies detected by NetworkMiner indicate a change in the MAC address for 172.16.1.39, aligning with the MAC address of IP 172.16.1.35. This discrepancy suggests a potential intrusion or security breach.

Figure 4: Anomaly

207.46.19.60 – The IP address is connected to the hostname “lb1.www.ms.akadns.net, g.www.ms.akadns.net, www.microsoft.com”. I infer that this is a redirection of a web server in which the user can be then sent back to MSN’s home page when pressed “here”.

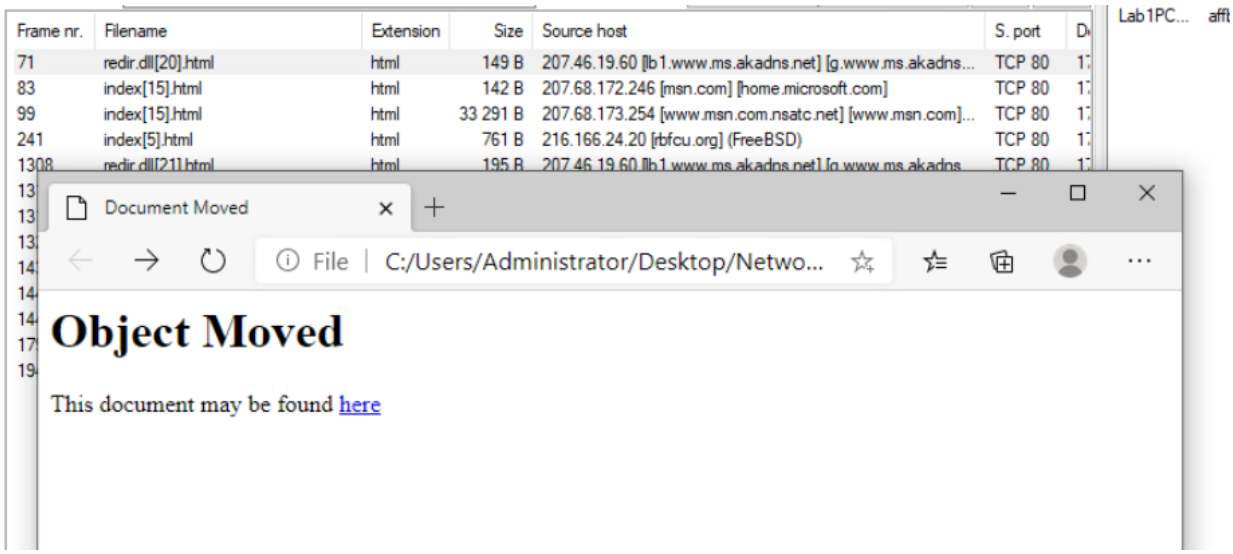


Figure 5: Redirection

Linux OS:

66.142.254.158 – This IP address is associated with the hostname “global.msads.net, hm.sc.msn.com.c.footprint.net, stb.msn.com”. Looking at the packets, this IP may be related to Microsoft advertising or MSN home page (global.msads.net),streaming services (Set-Top Box), and a specific subdomain of the footprint web server.

70.245.59.65 – The IP address is associated with three hostnames: "a943.x.a.yming.com," "a943.x.a.yming.com.georedirector.akadns.net," and "us.js1.yming.com." .What’s interesting is that when analyzing the TCP stream for host "us.js1.yming.com," the referrer was "http://us.f812.mail.yahoo.com/ym/login?rand=4uac50365fsjr."
These sparks interest specifically related to the specific domain on Yahoo!'s web server (a943.x.a.yming.com). The noteworthy aspect is the use of a geo redirector in the second hostname, "a943.x.a.yming.com.georedirector.akadns.net." This geo redirector facilitates redirection based on user geolocation (GeotargetingWP) and given the presence of 'us' in the subdomain, it does hint of a focus on users in the United States. I have inferred that this IP address is likely involved in Yahoo!'s mail service and that Mr. Kauffman may be sending an

email within the U.S., supported by the geolocation-based redirection provided by the geo redirector, and evidenced by the 'us' subdomain.

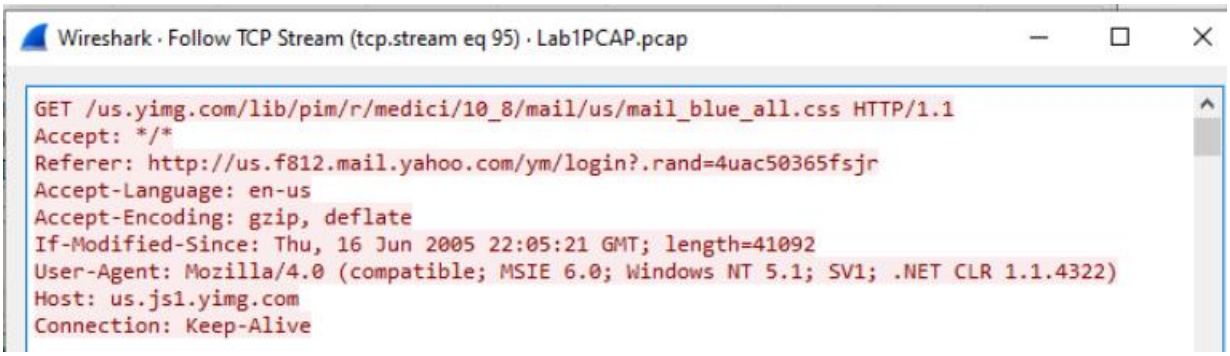


Figure 6: Yahoo!

70.245.59.14 – The IP address belongs to the same hostname associated with IP address 70.245.59.65 however, there are additional hostnames "…a321.x.a.yimg.com, us.js2yimg.com". The packets focus on the hostname "us.i1.yimg.com". This may be associated with sending a gif within the same email as in IP address 70.245.59.14. The reason for this is that the referrer matches up with the one wrote down previously.

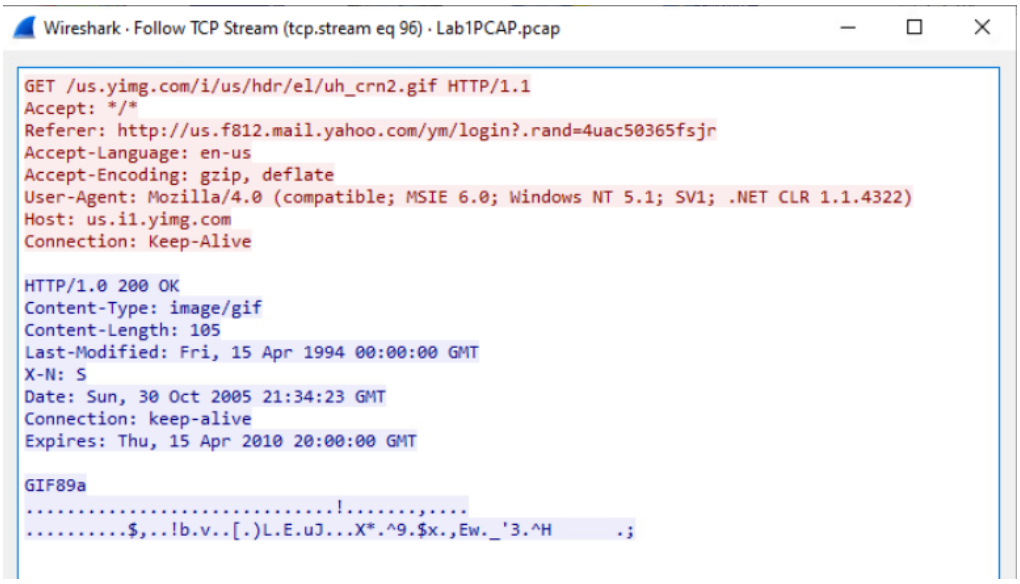


Figure 7: GIF

209.3.40.190 – The IP address belongs to the same hostname associated with IP address 66.142.254.158. However, the packets do focus on the hostname "stb.msn.com." As said previously STB is a streaming service which could mean that this IP address is associated with this type of media. In addition, we can also see that the content-type is "application/x-shockwave-flash which is an Adobe Flash file used for "multimedia, vector graphics and ActionScript (Wikipedia)."

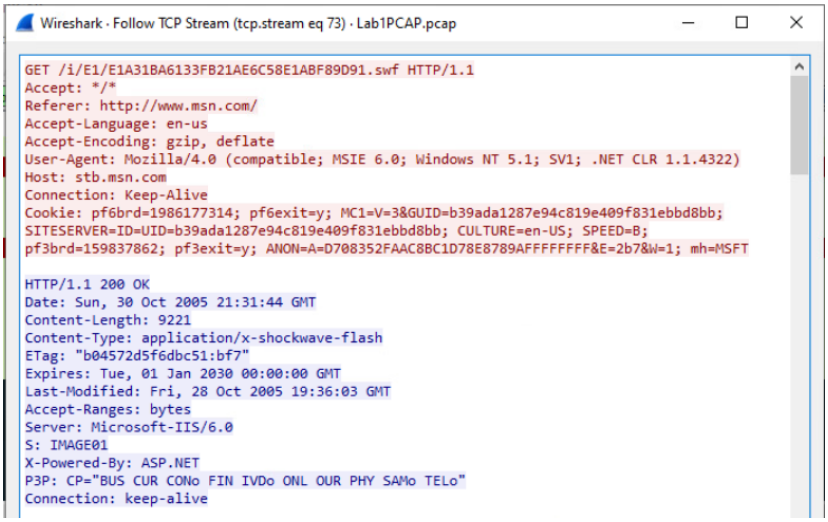


Figure 8: STB

70.245.59.31 – The IP address belongs to the same hostname associated with IP address 70.245.59.65 however, the hostname does not contain "us.i1.yimg.com." The packets focus on the hostname "us.js2.yimg.com". This may indicate the presence of JavaScript code associated with the Yahoo! Mail web application. This is evident in the TCP stream for content-type is "application/x-javascript. The MIME (Multipurpose Internet Mail Extensions) type

"application/x-javascript" is used to specify the encoding for files that contain JavaScript source code (MimeApplication). In addition, seeing that the referrer is different from the referrer as in the previous IPs this could be specific for the actual Yahoo mail application rather than the email being sent.

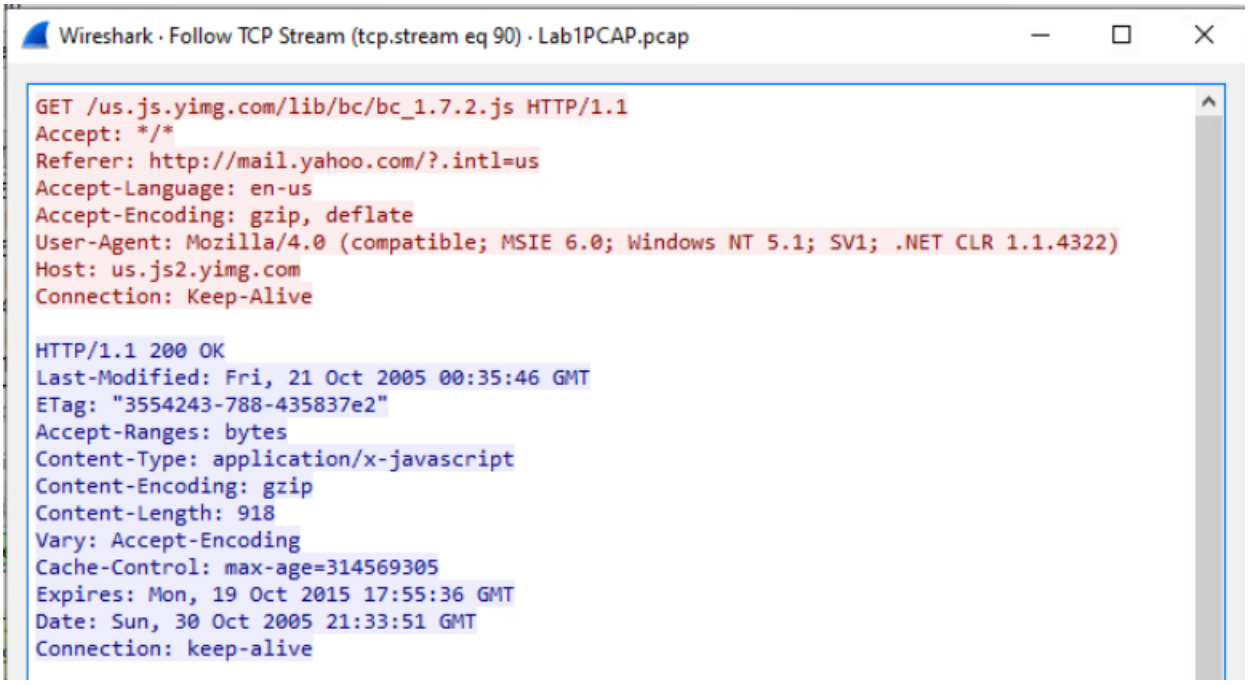


Figure 9: JavaScript

FreeBSD OS:

216.166.24.20 – This IP address is connected to the hostname “rbfcu.org, www.rbfcu.org”. The website associated with rbfcu is the Randolph-Brooks Federal Credit Union.

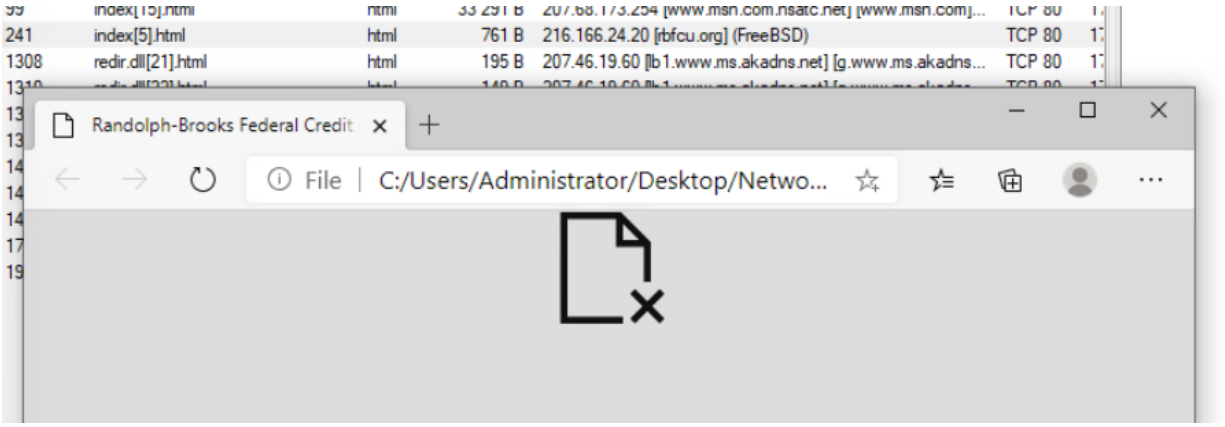


Figure 10: RBFCU

66.39.22.157 – This IP address is linked to the hostname “linux-wlan.org, ftp.linux-wlan.org”. It is associated with the Linux Wireless LAN website which is dedicated to providing support for wireless networking in the Linux operating system. In addition, looking at the packets there are many that use the ftp protocol, primarily designed for facilitating file transfers.

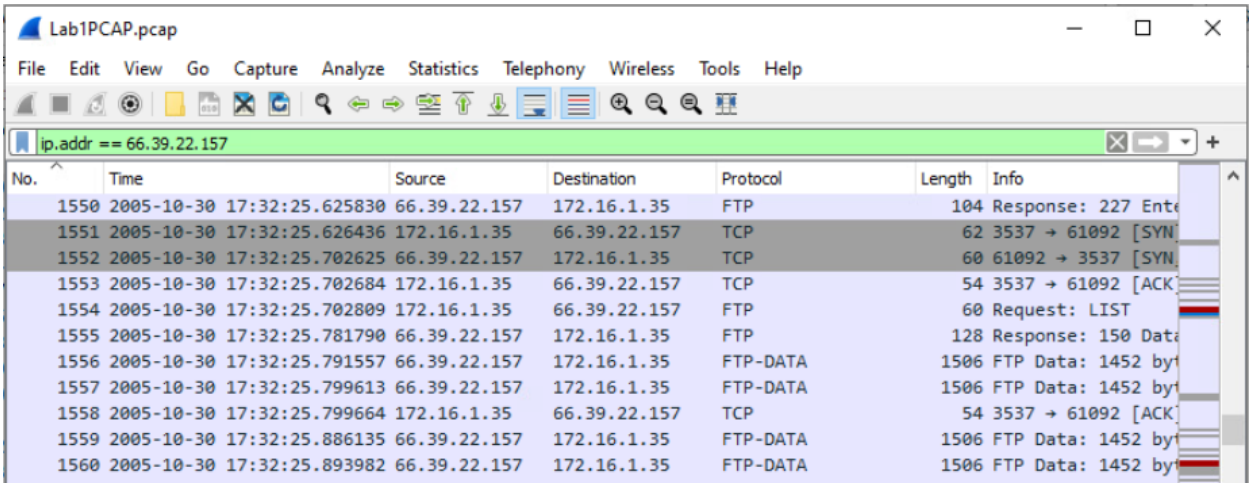


Figure 11: linux-wlan

206.190.37.187 – The hostname of this IP address is “f812.mail.yahoo.com, us.f812.mail.com”. This is linked to a yahoo email application that is on FreeBSD. Just as I talked about with the

yahoo email application on Windows, given the presence of 'us' in the subdomain, it does hint of a focus on users in the United States.

216.109.127.60 – The IP is assigned the hostname “login.yahoo.akadns.net, login.yahoo.com”. By looking at the hostname this IP address could be connected to the login page of yahoo.com. Seeing that there is a set cookie, specifically a HTTP cookie, suggests that it will “perform cookie-based authentication to maintain the session for each user.” (Gupta)

66.218.75.184 – The hostname assigned to this IP address is the same as the one above however it adds the additional hostname “mail.yahoo.com”. From looking at the hostnames it seems that there is a link to the login and mail services of yahoo. From the packets, I see that the “Cache-Control” is set to private meaning that the website is displaying private data, maybe the user specific information.

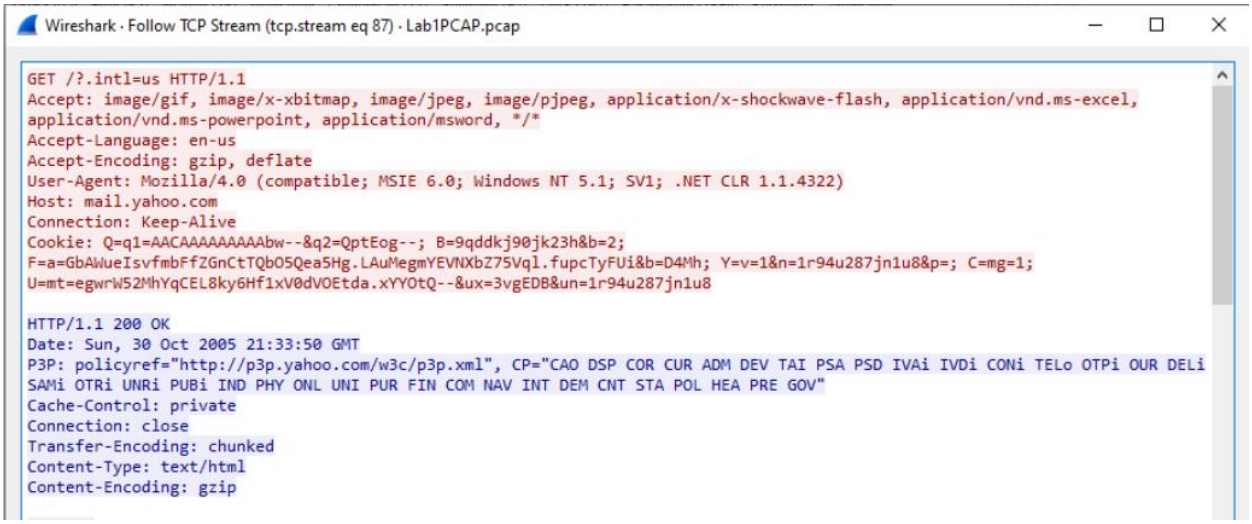


Figure 12: Private Cache

Unknown OS:

152.163.15.208 – The IP address has the hostname “2.internet.aol.com”, and “dial.internet.aol.com”. The host names could be a connection to AOL (America Online) services. AOL provides internet services, including dial-up access, which aligns with the "dial.internet.aol.com" hostname. The "2.internet.aol.com" could represent a specific server or service within AOL's server. In the late 90’s and early 2000’s AOL provided internet users email and instant messaging services (Britannica).

172.16.0.1 – The hostname is “homeportal.gateway.2wire.net”. This is likely associated with a home networking gateway or router. The "2wire.net" domain indicates that it may be a device manufactured by 2Wire, a company that provides broadband products, software, and service platforms to carriers.

207.68.173.254 – Hostname for this IP address is “www.msn.com.nsatc.net” and “www.msn.com”. This could be a specific subdomain of the Microsoft Network web server. The reason I suspect this is that the host name in the packets is 'www.msn.com'. There could also be a login attempt by a user seeing that is uses HTTP Cookie and a private cache control.

129.115.102.173 – This hostname is “ruby1604.utsa.edu”. This appears to be a specific email of a user. This IP address is linked to a server or device with the name "ruby1604" within the domain "utsa.edu”.

172.16.1.37 – This IP address is associated with the hostname “DVR-8525.local”. Looking at the packets it does look like it’s associated with TiVo Media Service.

66.218.70.70 – IP is assigned the hostname “ssl.vip.scd.yahoo.com” and “sec.yimg.com”. These hostnames hint that they can be associated to a specified Yahoo! application(s).

68.142.213.132 – The IP address is linked to the hostname “bc.us.yahoo2.akadns.net, bc.us.yahoo.com”, indicating a connection to Yahoo. The "akadns.net" part of the hostname indicates the use of Akamai, a content delivery network. Given that the referrer is "http://mail.yahoo.com/?.int1=us," it strongly suggests that the connection is related to Yahoo Mail services.

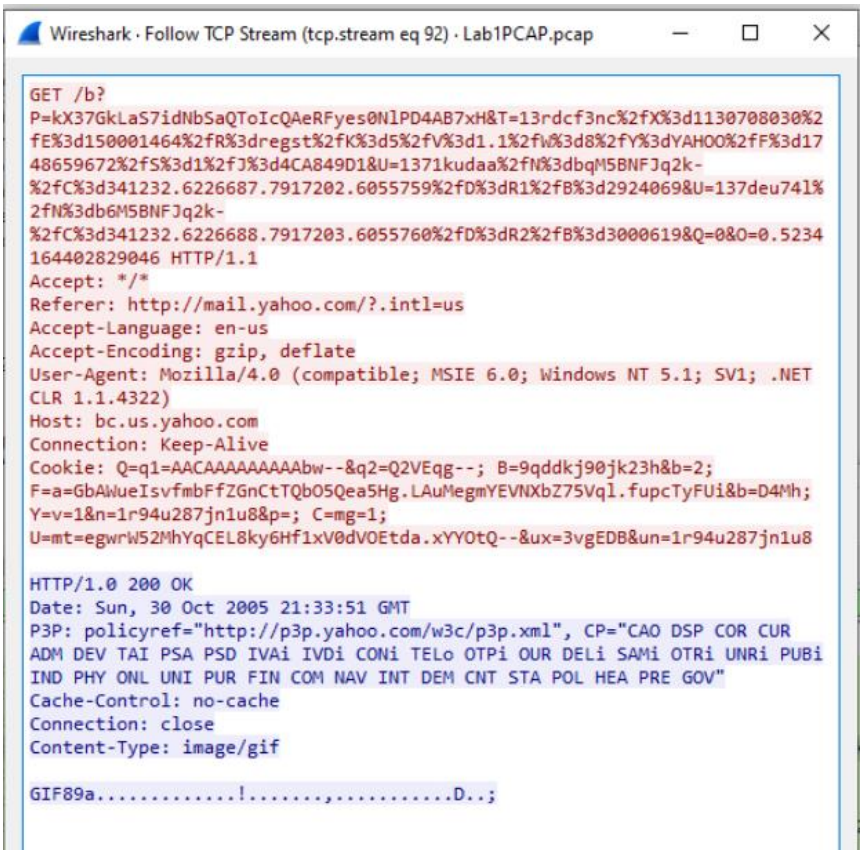


Figure 13: Mail

64.12.15.121 – This IP address has the host name “10.internet.aol.com” and “dial.internet.aol.com”. Just as the IP address 152.163.15.208 the host names can be a connection to AOL (America Online) services.

152.163.5.135 – Hostname assigned to this IP address is “ipt-rtce07.dial.aol.com”. Here we have another AOL connection. In addition, “dial” subdomain could reference AOL’s dial-up service.

Summary: I've examined the primary hosts in the system, and the remaining IP addresses share similarities with those already discussed. Notably, there are two distinct ones: the broadcast IP address and the multicast IP address. It's crucial to raise a red flag for anything not associated with email, as Mr. Kaufman explicitly mentioned that his network is solely for email use. The IP address causing concern is the second host impersonating Mr. Kaufman (172.16.1.39), along with the banking service (66.39.22.157), the linux-wlan involved in file transfers (66.39.22.157), and the device with the hostname ruby160.utsa.edu (129.115.102.173).

Analysis of PCAP:

Here I will break down some of the packet streams related to the IP addresses that have triggered concerns.

The second host impersonating Mr. Kaufman (172.16.1.39)

An interesting thing about this stream is that on packet 43 the MAC address for IP address 172.16.1.39 is different (00:0f:66:15:06:14) from what is displayed in frame 56 (down below). As you can see the MAC address is the same MAC address as Mr.Kaufman's device. This means that despite the fact that the traffic in this pcap is associated with Mr.Kaufman's IP address it cannot be trusted. It is safe to assume that anything that's not email is initiated by this intruder.

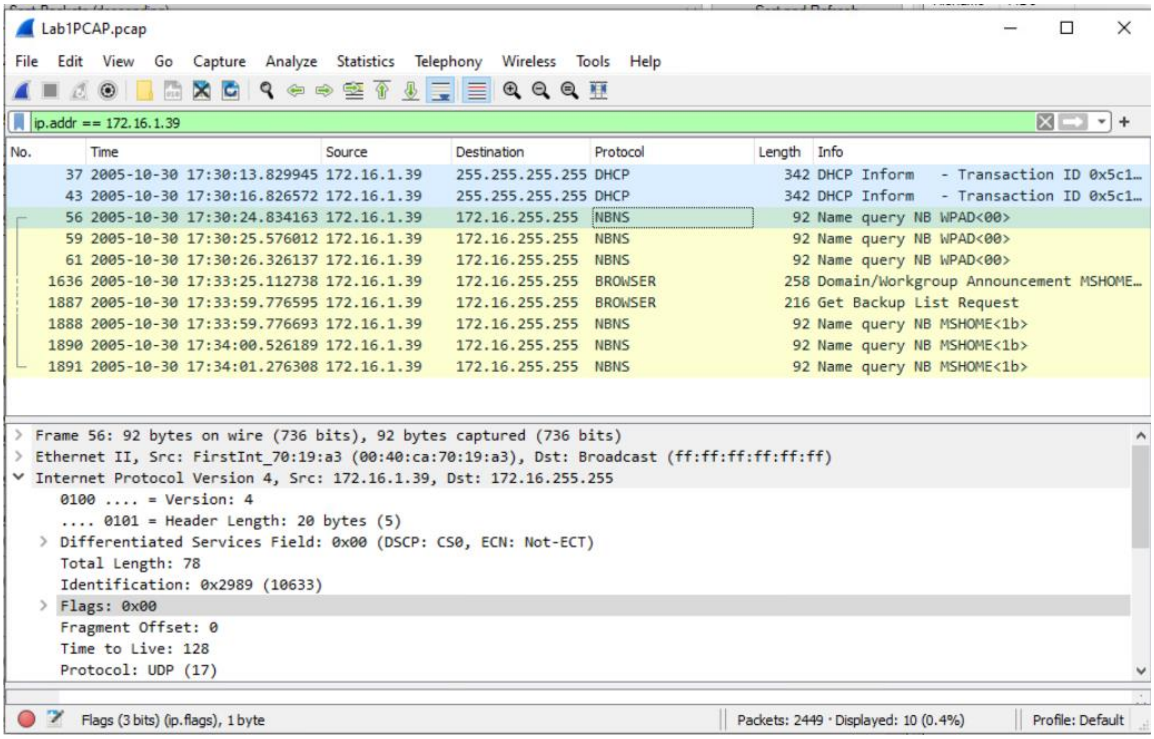


Figure 14: Kaufman 2.0

Banking service (216.166.24.20)

Analyzing the packet streams for the specified IP address, a notable transition is observed between TCP stream 8 through 57 and 66, which primarily involves website coding elements, and TCP stream 58 through 65. The first set of streams encompasses aspects like button images and HTML code for the welcome page. However, the second set presents an interesting shift as SSLv3 and SSLv2 protocols come into play. Wireshark's output reveals references to "RSA Data Security" and "Secure Certification Authority."

This transition introduces a challenge as the packets transform from visible output and informational content to encrypted texts. By doing some outside research I was able to find that banks use SSL “when you sign in to online banking, all of your data is fully encrypted using SSL (ScotiaBank).” Furthermore, SSL serves the critical purpose of maintaining the privacy of transferred data, guaranteeing a secure online banking session. Considering this, the observed packets could be linked to the intruder attempting to log into an account, potentially accessing sensitive information such as Mr. Kaufman's banking statements.

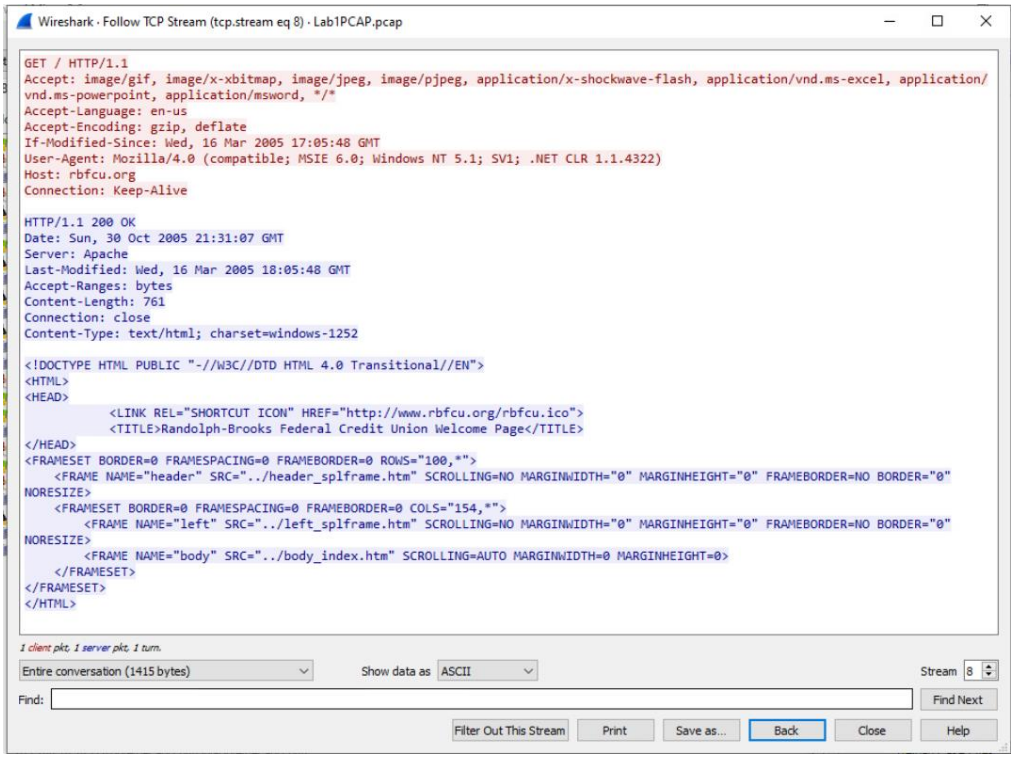


Figure 15: RBFCU - HTML

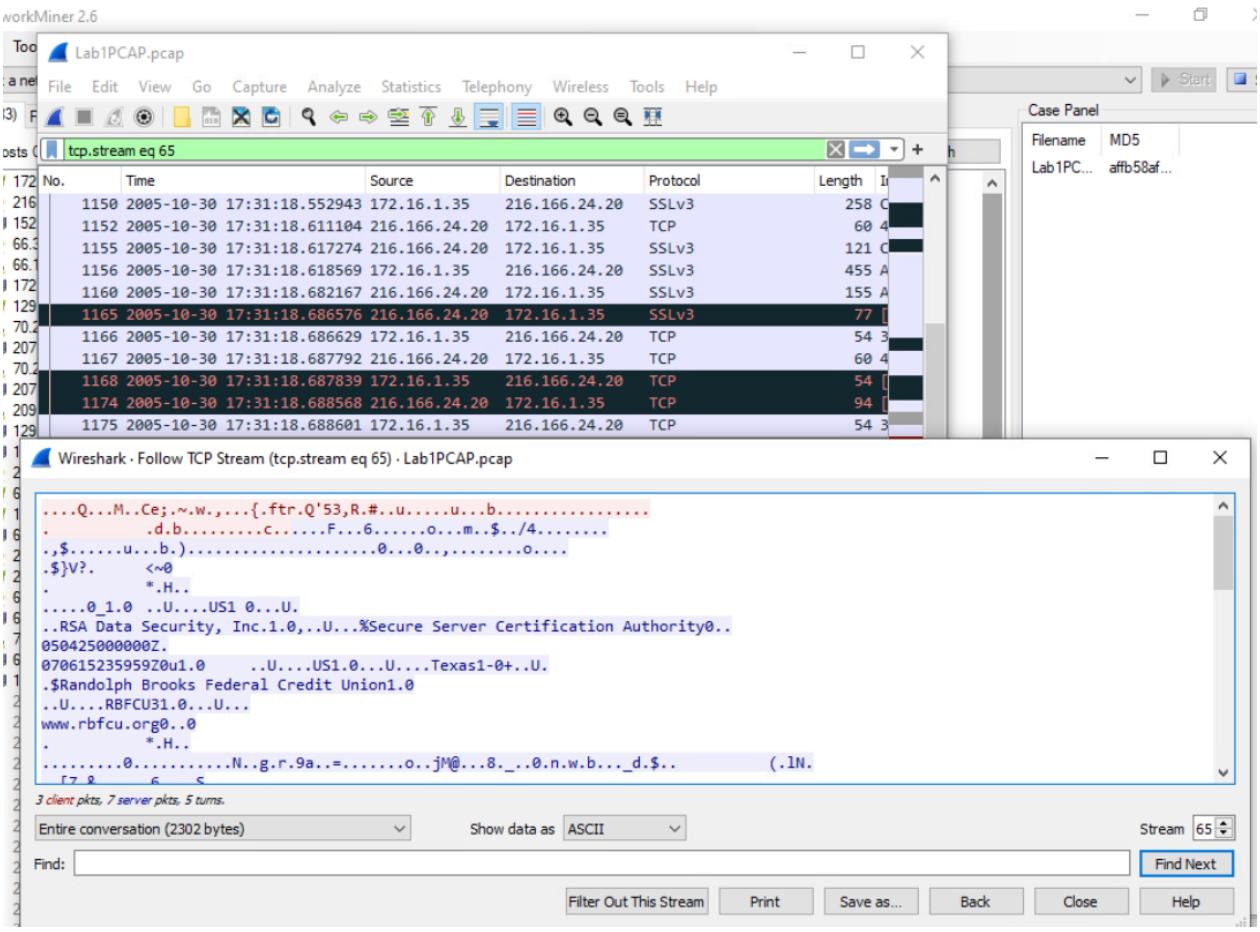
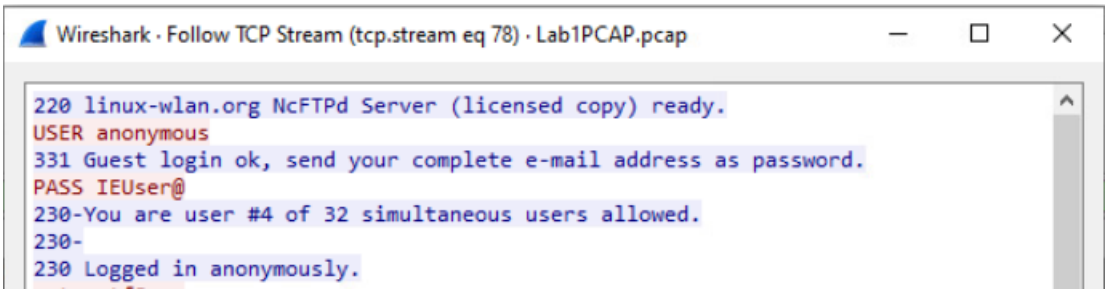


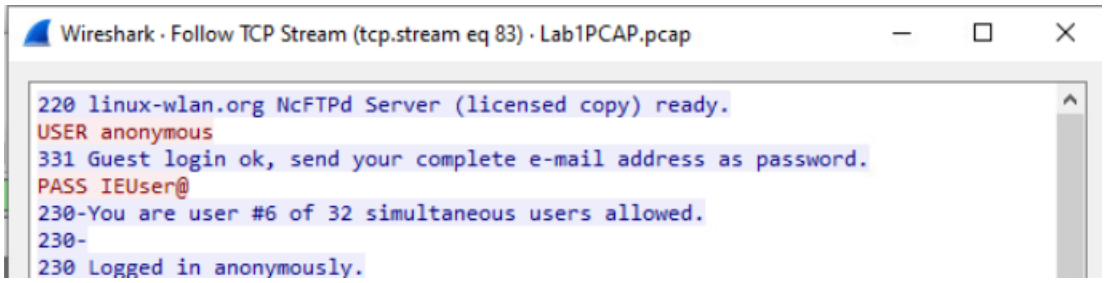
Figure 16: RBFCU - SSL

Linux-wlan involved in file transfers (66.39.22.157)

Looking at these packets they are split into two kinds of streams, one for the FTP protocol and one for FTP-Data protocol.

In the FTP protocol, the intruder initiates four logins into the NcFTPd Server, employing the same login credentials each time. NcFTPd is a UNIX-based software server designed for high-performance File Transfer Protocol, capable of facilitating simultaneous data transfers for multiple users. Upon anonymous login, the intruder executes various commands to explore the server, including "syst," "site help," and "PWD." Afterwards, the intruder changes the directory using the command "CWD /pub/linux-wlan-ng/." The "TYPE A" command is employed to set the transfer type to ASCII, while the "PASV" command requests the server to enter passive mode for data transfers. Notably, due to the setting of "PASSIVEIGNOREADDR" to True, as per IBM, data is transmitted via the port assigned by the server but disregards the IP address and instead sends it to the address used for logging into the NcFTPd server (IBM). Finally, the "LIST" command is utilized to transfer information through the established connection.





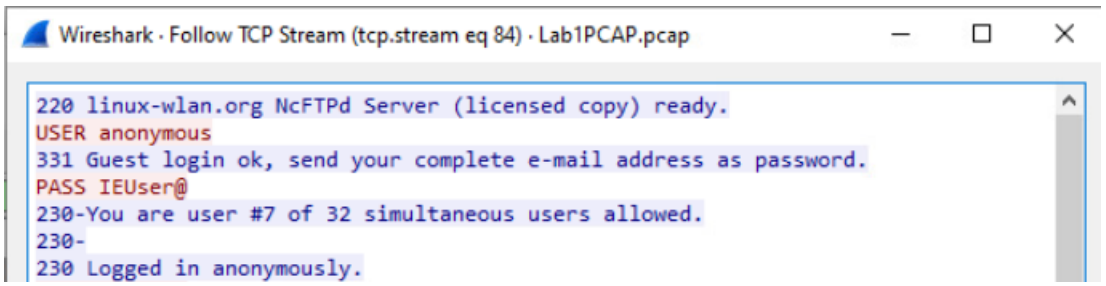


Figure 17-20: FTP

The repetition of the same login, commands, and file transfer across multiple accounts strongly suggests that this could be a script, or an automated process being executed by the user.

In the second part of the stream, the FTP-DATA protocol is evident, representing the packets containing the files transferred by the intruder. The visual representation below indicates the successful transmission of data. However, considering that the message is directed to Mr. Kaufman's IP address, and given the shared MAC address with the intruder, there is a potential risk of data interception during transmission.

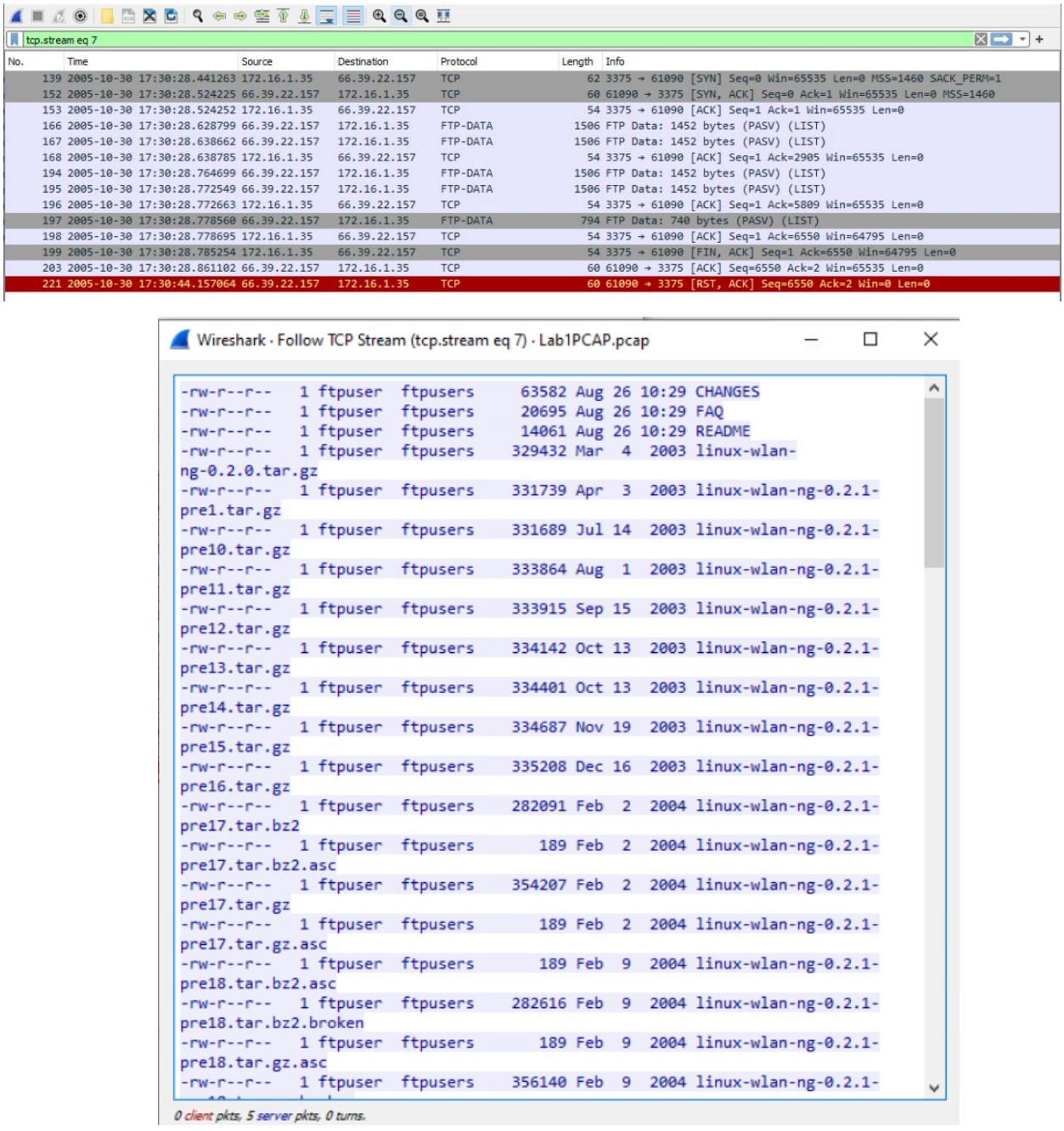


Figure 20-22: FTP-DATA

Device with the hostname ruby160.utsa.edu

Examining the device with the hostname "ruby160.utsa.edu," the packet analysis reveals the usage of SSLv2 and SSLv3 protocols. This device appears to be linked to a UTSA web server, possibly associated with mail services based on its hostname. Despite limited activity recorded for this user, there might be a connection to the intruder due to the fact that the IP that made this connection was Mr.Kaufman. However, considering Mr.Kaufman's statement about using the network solely for email, the observed association with him remains limited. This may not be malicious however may need to be removed from the network.

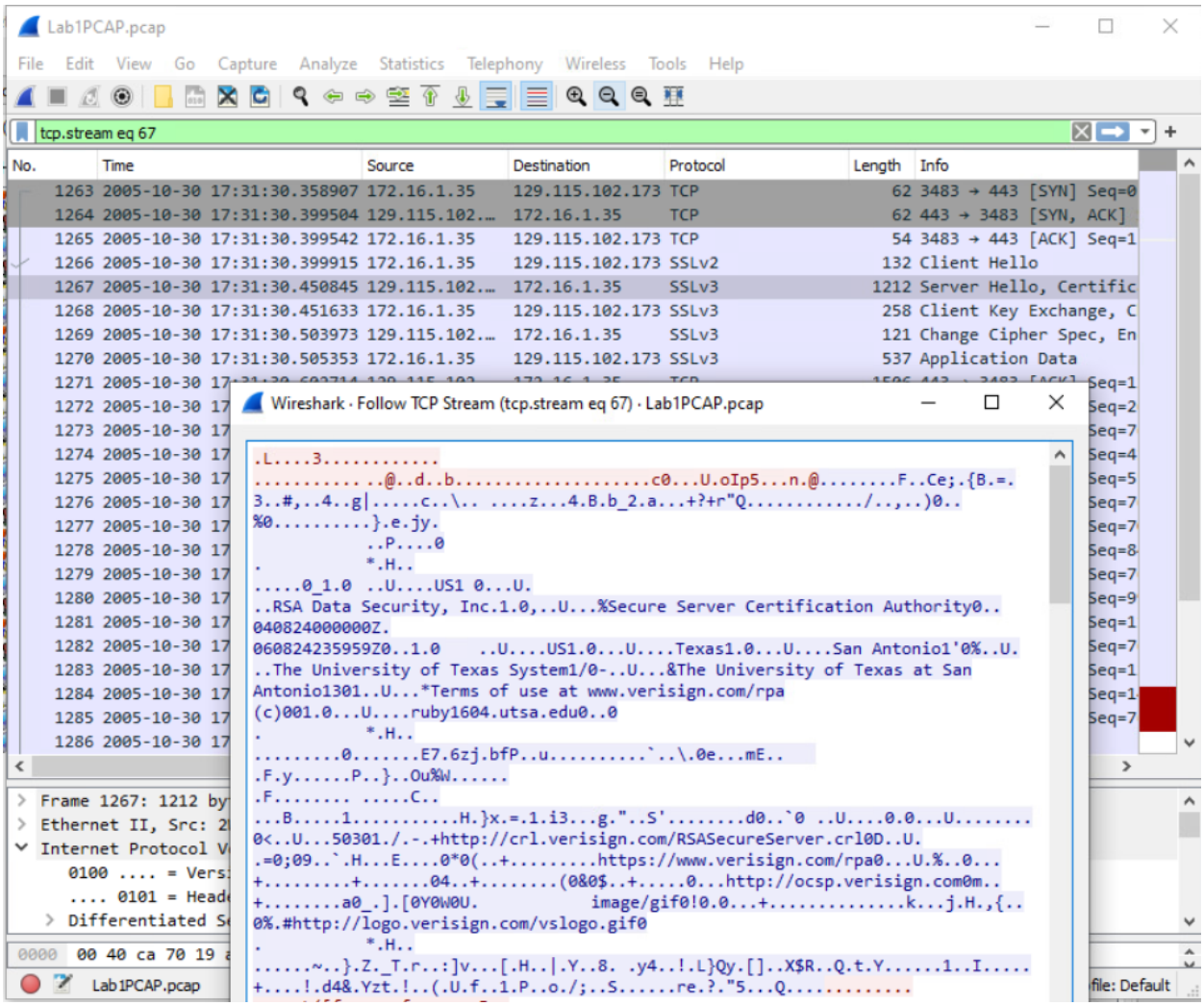


Figure 23: ruby160

The Story:

In my examination of the packet data, I've uncovered several interesting incidents, notably the presence of a suspicious user who utilized MAC address spoofing to mirror Mr. Kaufman's MAC address. It appears plausible that this user gained entry to the network through a phishing attack specifically targeting Mr. Kaufman. This assumption is based on Mr. Kaufman's exclusive use of the network for email activities. The potential entry point for the intruder could have been if Mr. Kaufman unintentionally interacted with a deceptive email designed for the intruder to infiltrate the network and replicate his MAC address. Subsequently, the intruder had the capability to carry out various actions.

Among these actions, the intruder successfully accessed files and executed transfers using an NcFTPd server. My observation of the packets reveals that the attacker performed this task four times with distinct accounts, consistently running the same commands. This pattern suggests that the intruder automated these actions. Additionally, based on the available evidence, the data was directed to Mr. Kaufman's IP address, indicating that the intruder intercepted it before reaching the intended destination.

The intruder successfully gained access to a bank, and I suspect that it may be related to Mr. Kaufman's account. My reasoning for this suspicion is rooted in the possibility that if the intruder accessed the network via email phishing, they could have read a bank-related email and obtained a password, either through a reset link or from a file. Upon reviewing the packet information, I noticed that the data theft occurred before the packets associated with the bank activities. This has led me to consider the likelihood that the stolen data might contain passwords.

The actions carried out by the intruder were malicious, indicating a clear intent to steal private data from Mr. Kaufman.

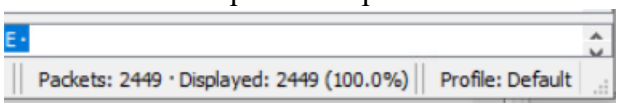
I have observed some events that are less malicious, such as the device with the hostname "ruby160.utsa.edu." This device seems to be connected to a UTSA web server, potentially linked to mail services based on its hostname. Although there is limited activity recorded for this user, there could be a connection to the intruder since the IP making this connection belongs to Mr. Kaufman. However, given Mr. Kaufman's statement about using the network exclusively for email, the observed association with him remains restricted. While it may not be malicious, consideration should be given to removing it from the network.

2) Perform an analysis on the captured traffic. Some things you should consider are the following (not all of
these happened and may not be all inclusive either):

a. **How long did the session capture last?**
   Seeing that the start of the packets occurred at 5:29:35.072629 and ended at 5:38:00:00.770109 the session lasted about 8 mins and 26 seconds

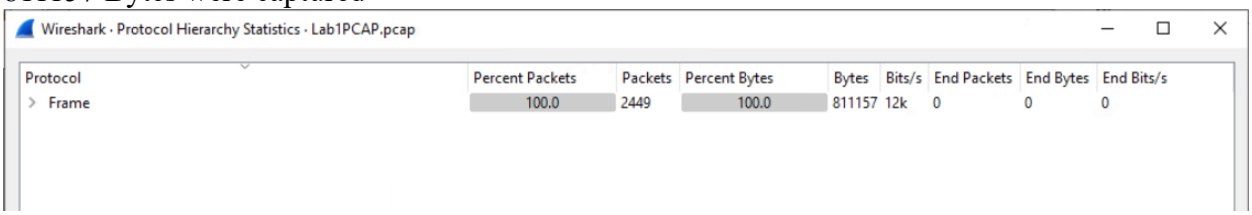
b. **How many packets were captured?**

   There were 2449 packets captured

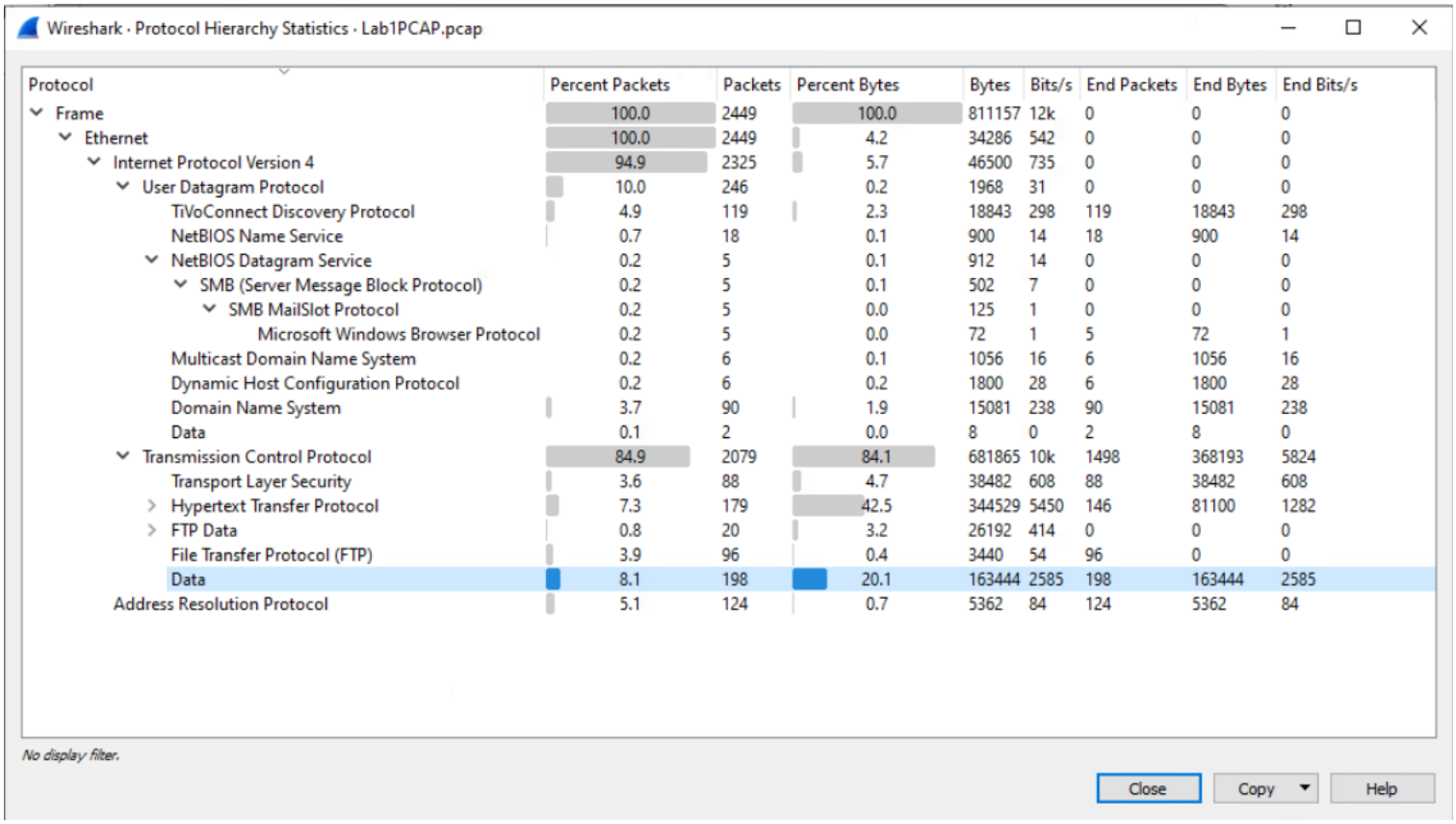


c. **How many bytes were captured?**

   811157 Bytes were captured



d. What protocols were observed?



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2449	100.0	811157	12k	0	0	0
Ethernet	100.0	2449	4.2	34286	542	0	0	0
Internet Protocol Version 4	94.9	2325	5.7	46500	735	0	0	0
User Datagram Protocol	10.0	246	0.2	1968	31	0	0	0
TiVoConnect Discovery Protocol	4.9	119	2.3	18843	298	119	18843	298
NetBIOS Name Service	0.7	18	0.1	900	14	18	900	14
NetBIOS Datagram Service	0.2	5	0.1	912	14	0	0	0
SMB (Server Message Block Protocol)	0.2	5	0.1	502	7	0	0	0
SMB MailSlot Protocol	0.2	5	0.0	125	1	0	0	0
Microsoft Windows Browser Protocol	0.2	5	0.0	72	1	5	72	1
Multicast Domain Name System	0.2	6	0.1	1056	16	6	1056	16
Dynamic Host Configuration Protocol	0.2	6	0.2	1800	28	6	1800	28
Domain Name System	3.7	90	1.9	15081	238	90	15081	238
Data	0.1	2	0.0	8	0	2	8	0
Transmission Control Protocol	84.9	2079	84.1	681865	10k	1498	368193	5824
Transport Layer Security	3.6	88	4.7	38482	608	88	38482	608
Hypertext Transfer Protocol	7.3	179	42.5	344529	5450	146	81100	1282
FTP Data	0.8	20	3.2	26192	414	0	0	0
File Transfer Protocol (FTP)	3.9	96	0.4	3440	54	96	0	0
Data	8.1	198	20.1	163444	2585	198	163444	2585
Address Resolution Protocol	5.1	124	0.7	5362	84	124	5362	84

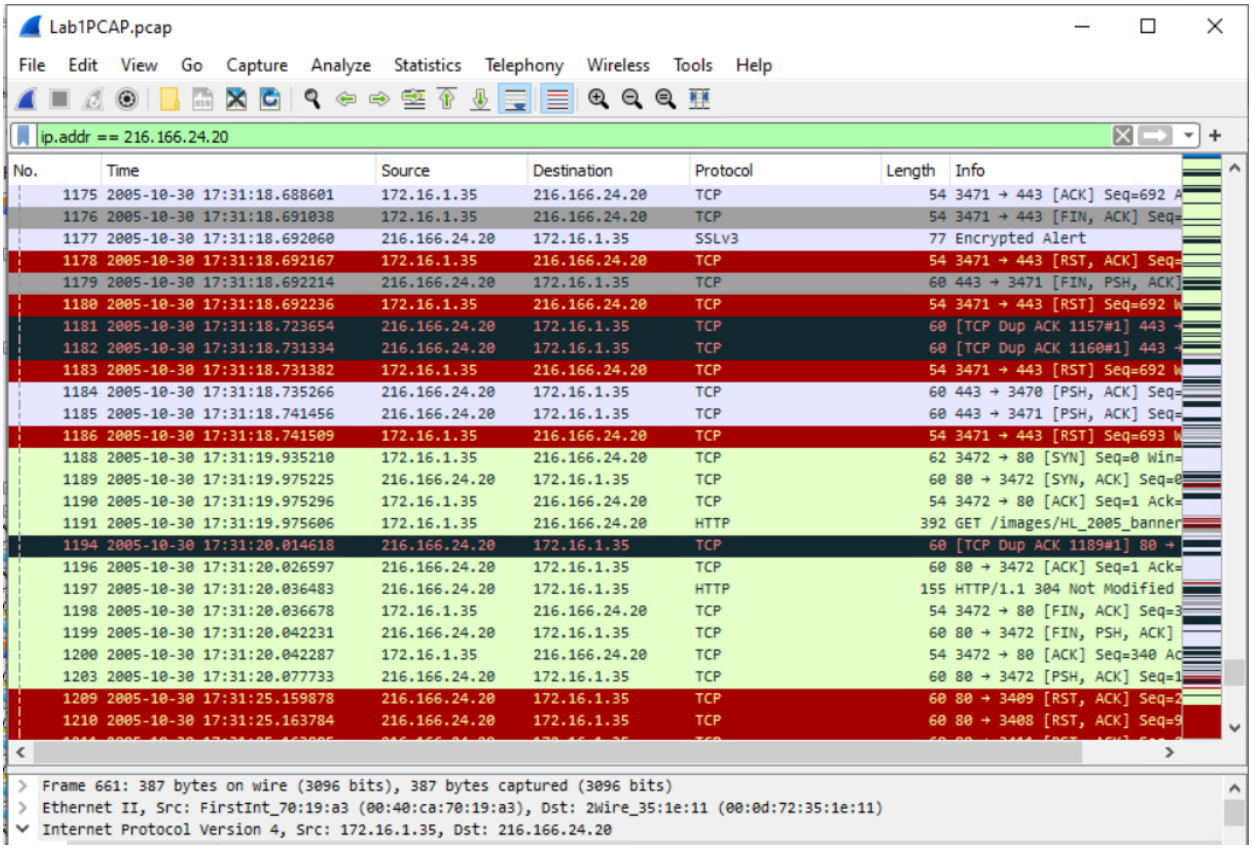
e. When did the bulk of the data get transmitted?

The bulk of the data got transmitted from 17:31:12:931233 – 17:31:37:460605. This IP address is connected to the bank site that the intruder logged into

172.16.1.35	209.3.40.190	31	11k	15	1396	16	10k	53.361763	130.5376
172.16.1.35	216.166.24.20	1,014	210k	455	48k	559	162k	94.113124	28.2749
172.16.1.35	216.109.127.60	18	5233	9	1877	9	3356	285.230051	17.5858

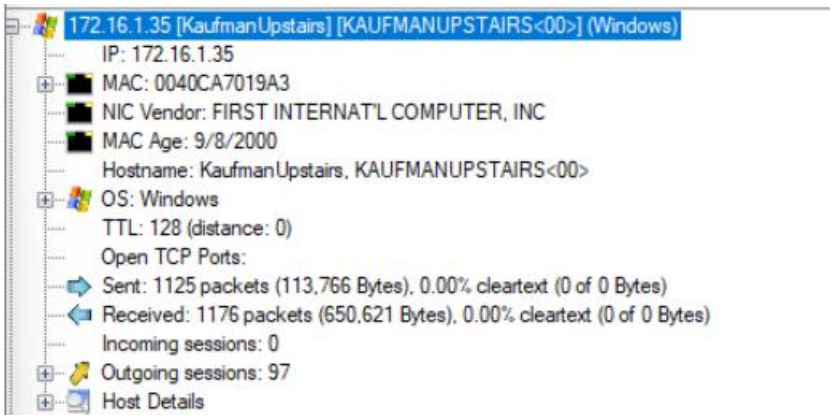
f. What caused this transmission spike?

The spike in transmission can be attributed to errors in TCP flags and the occurrence of reset packets.



g. What is the name of the host computer? It's IP address?

The host name is "Kaufman Upstairs, KAUFMANUPSTAIRS<00>" and the IP associated with it is 172.16.1.35



h. What Operating system is it using?

The Operating System the host is using is Windows. The operating system's the other host are using are FreeBSD and Linux.

i. What does the local network look like?

Answer can be found under the "Network Mapping".

j. What device names are on the local network?

Answer can be found under the "Network Mapping".

k. Are any other devices on the network?

Answer can be found under the "Network Mapping".

Citations:

Tools for this lab

Breeden, John. “What is Wireshark?” Network World, 8 June 2022, https://www.networkworld.com/article/971145/what-is-wireshark.html. Accessed 3 February 2024.

Netresec. “NetworkMiner - The NSM and Network Forensics Analysis Tool.” Netresec, https://www.netresec.com/?page=NetworkMiner. Accessed 3 February 2024.

Wireshark. “Chapter 1. Introduction Prev Next.” Wireshark, https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs. Accessed 3 February 2024.

Analysis

Bhardwaj, Rashmi. “TCP FIN vs RST Packets- Know the Difference - IP With Ease.” IPWITHEASE, 19 September 2020, https://ipwithease.com/tcp-fin-vs-rst-packets/. Accessed 11 February 2024.

Britannica. “AOL | American Online Company.” Britannica, 19 December 2023, https://www.britannica.com/topic/AOL. Accessed 9 February 2024.

editorialtoday.com. “Importance Of SSL Certificates On Banking Websites.” Street Directory, https://www.streetdirectory.com/etoday/-eacpjj.html. Accessed 10 February 2024.

GeotargetingWP. “🌎 Geo Redirects WordPress plugin.” Geotargeting WP, https://geotargetingwp.com/geo-redirects. Accessed 9 February 2024.

Gupta, Deepak. “Cookie-based vs. Cookieless Authentication: What's the Future?” LoginRadius, https://www.loginradius.com/blog/engineering/cookie-based-vs-cookieless-authentication/. Accessed 9 February 2024.

IBM. YouTube: Home, 9 November 2017, https://www.ibm.com/docs/en/zos/2.3.0?topic=messages-eza2403i. Accessed 10 February 2024.

Kaspersky. “What is an SSL Certificate & Why is it important?” Kaspersky, https://usa.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate. Accessed 10 February 2024.

MimeApplication. “mime application/x-javascript.” Mime types database, https://mimeapplication.net/x-javascript. Accessed 9 February 2024.

NcFTP. “NcFTPd Server: FTP Server Software for UNIX.” NcFTP Software, https://www.ncftp.com/ncftpd/. Accessed 11 February 2024.

netify. “akadns.net - Domain Info.” Netify, https://www.netify.ai/resources/domains/akadns.net. Accessed 9 February 2024.

PitchBook. “2Wire Company Profile: Valuation, Investors, Acquisition.” PitchBook, https://pitchbook.com/profiles/company/13211-74#overview. Accessed 9 February 2024.

ScotiaBank. “Are my online banking transactions secure by using SSL? - Scotiabank Help Centre.” Help Centre - Scotiabank Help Centre, 2 July 2020, https://help.scotiabank.com/article/are-my-online-banking-transactions-secure-by-using-ssl. Accessed 10 February 2024.

TechMonitor. “What is AOL?” Tech Monitor, 3 January 2023, https://techmonitor.ai/what-is/what-is-aol-4984420. Accessed 9 February 2024.

Villanueva, John Carl. “Active vs. Passive FTP Simplified: Understanding FTP Ports | JSCAPE.” jscape, 16 November 2023, https://www.jscape.com/blog/active-v-s-passive-ftp-simplified. Accessed 11 February 2024.

Wikipedia. “SWF.” Wikipedia, https://en.wikipedia.org/wiki/SWF. Accessed 9 February 2024.

Wireshark. “Wireshark Q&A.” Wireshark Q&A, 7 March 2013, https://osqa-ask.wireshark.org/questions/19274/how-to-know-how-much-data-transfer-occurred-in-captured-pcap-file/. Accessed 11 February 2024.