Lab 3: Network Sniffing

Procedure

Part 1, *first screenshot*:

- Downloaded and installed Wireshark and rebooted my computer once Wireshark was installed.
- Opened Wireshark application and put it into capture mode on my Wi-Fi.
- Went to my browser (Edge) and typed a random domain name that doesn't exist and tried to connect http://www.jahfjrigjfjdivobofkjhkd.com.
- Opened a terminal.
- Then I typed: ping www.google.com and then enter via PowerShell.
- Visited www.amazon.com and click on "sign in" (but did not sign in).
- Stopped packet capture.
- Applied a simple filter, *dns*, to display DNS packets, took a screenshot of the results, and pasted into my PowerPoint presentation (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide one*).

Part 2, *second screenshot*:
Found the DNS packets for the website that doesn't exist (*http://www.jahfjrigjfjdivobofkjhkd.com*) and located in the Domain Name System (response) by applying *dns.qry.name contains www.jahfjrigjfjdivobofkjhkd.com* filter. Here I observed the first packet and the sixth packet. I know the first packet is the request and sixth packet is the response based on their transaction IDs, *0x3011* (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide two*).

Part 3, *third screenshot*:

- Removed the DNS packet filter.
- Applied a filter, *icmpv6*, to display ICMP packets, took a screenshot of the filtered results, and pasted in my PowerPoint presentation (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide three*).

Part 4, *fourth screenshot*:
Found the ICMP packets that contained the ping data I sent, took a screen capture and pasted into my PowerPoint presentation (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide four*). I analyzed and compared the Source and Destination contents, specifically the IPv6 addresses, via Wireshark to the IPv6 address in the terminal. I noticed the same IPv6 address in both the packet list pane and in the terminal.

Part 5, *fifth screenshot*:

- Found the first TLS x.x "Client Hello" packet associated with the IP address for www.amazon.com.
- Expanded packet contents and under "Transport Layer Security," drilled down to find the list of cipher suites supported and took a screen capture and pasted it into my PowerPoint presentation (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide five*).

Part 6, *sixth screenshot*:

- Opened the "Lab 3 Capture" pcap file, provided by instructor, in Wireshark
- In Wireshark, selected "Edit," then "Find Packet," then pasted the hex values for a PDF file in the search bar and selected "Hex value" from the drop-down display then clicked "Find."

- Right clicked on the packet that contains the hex values for a .pdf file header, selected "Follow," then "TCP Stream."
- In the "Show data as" window, selected "Raw." Then selected "Save as" and saved file to my desktop with filename "capture" and with a .pdf extension.
- Took a screenshot of the saved file and pasted it into my PowerPoint presentation (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide six*).

Part 7, *seventh screenshot*:
Opened the file as a .pdf, took a screenshot of it opened and pasted it into my PowerPoint presentation (*reference separate file, ng_raymond_IS3513_Lab 3.pptx, slide six*).

Questions for this Lab Exercise

1. What is the Domain Name System (DNS)? What would happen if the DNS didn't function properly?

DNS is an important part of the internet infrastructure. Think of it as sort of like a phone book of the internet (*GoDaddy, 2023*). DNS translates domain names into numerical IP addresses that computers use to identify each other on a network. DNS works through a hierarchy of nameservers, from root nameservers, through top-level domain nameservers, down to authoritative nameservers for specific domains. When you type a URL into your web browser, it asks your internet service provider's DNS server to find the corresponding IP address. If your ISP's DNS server doesn't know the address, it will query other DNS servers up the hierarchy until it finds one that does.

If the DNS didn't function properly, it would essentially disrupt the internet. When a user enters a URL into a browser, a non-functioning DNS would not be able to translate that URL into an IP address. This means that the browser wouldn't know where to find the website the user is attempting to visit. Essentially, without DNS, every user would need to remember and enter the numerical IP addresses for each website, which is not practical or user-friendly.

2. What is the purpose of ICMP?

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is primarily used by network devices, like routers, to send error messages and operational information indicating whether a requested service is available, or a requested route is accessible *(Lutkevich, 2023)*. ICMP can be utilized to relay query messages, for instance, to check if a host is up or network-available (known as a "ping" like how I pinged for www.google.com in this lab). Although it's not used for sending application data, ICMP provides necessary functionality for managing and troubleshooting an IP network.

3. What is TLS? Which version did you observe in your packet capture?

Transport Layer Security (TLS) is a cryptographic protocol used to secure communications over a network (*Cloudflare, n.d.*). It provides privacy and data integrity between two communicating applications, and it's widely used for internet communications across web browsers and servers, email, instant messaging, and voice-over IP (VoIP).

In this lab I observed TLSv1.2. TLSv1.2 refers to version 1.2 of the TLS protocol. TLSv1.2 introduces some improved features compared to its predecessors, including the expansion of support for cryptographic algorithms and enhanced security (*Keycdn, 2022*). For example, it deprecated the use of MD5 and SHA-224 cryptographic hash functions due to identified vulnerabilities (*Keycdn, 2022*). Also, TLSv1.2 made the use of extensions more flexible.

4. Is there a Wireshark filter that could have saved you time in finding the "Client Hello" packet and cipher suites? What is it?

Yes, *tls.handshake.type == 1 (W3schools, 2023*).

5. What is FTP? How are you able to capture the contents of a .pdf using Wireshark in this example?

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another over the internet (*Kerner & Burke, 2021*). FTP is built on a client-server model architecture using separate control and data connections between the client and the server. It uses clear-text—unencrypted—transmission, which means that all the data including the usernames, passwords, and content are sent in a form that is easily readable (*JavaTPoint, n.d.*).

Wireshark is a network protocol analyzer that allows users to inspect data packets transferred over a network. When a file is transferred using FTP—with the understanding FTP is unencrypted—Wireshark captures the individual packets containing the file data. For the PDF files, I assess Wireshark users can find the relevant packets for the file transfer by looking for the FTP RETR (retrieve) or STOR (store) command in the packet details, which includes the filename. By following the TCP stream, I isolated the data packets specific to the PDF file. Wireshark provided an option to view this stream as 'Raw' data, and this raw data can then be saved as a PDF file. This may not work for encrypted files.

References

Cloudflare. (n.d.). *What is TLS (Transport Layer Security)?* Retrieved from Clouflare: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

GoDaddy. (2023). *What is DNS?* Retrieved from GoDaddy: https://www.godaddy.com/help/what-is-dns-665

JavaTPoint. (n.d.). *FTP*. Retrieved from JavaTPoint: https://www.javatpoint.com/computer-network-ftp

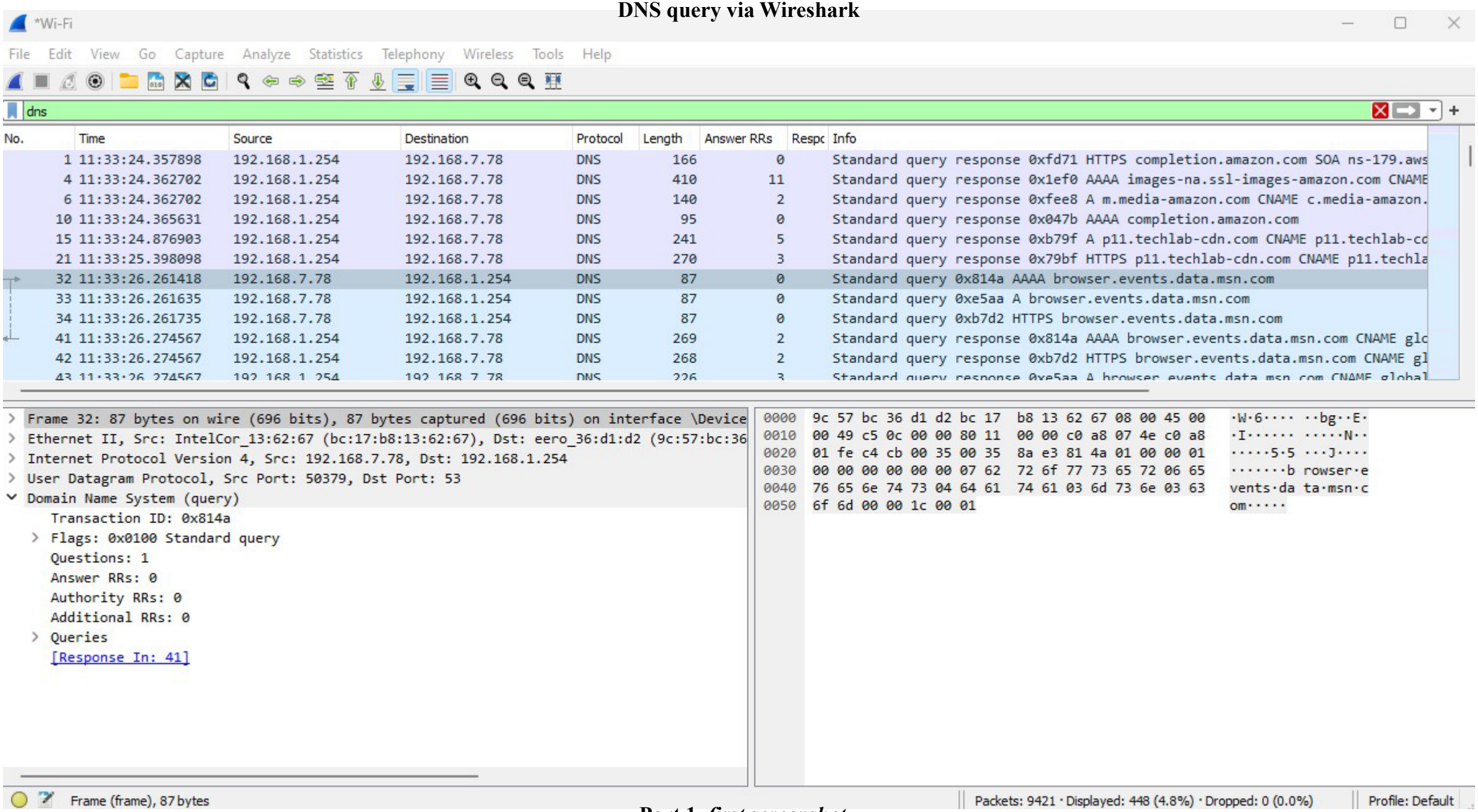
Kerner, S. M., & Burke, J. (2021, May). *FTP (File Transfer Protocol)*. Retrieved from TechTarget: https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP?Offer=abMeterCharCount_ctrl

Keycdn. (2022, February 22). *TLS 1.2 vs TLS 1.1*. Retrieved from https://www.keycdn.com/support/tls-1-2-vs-tls-1-1

Lutkevich, B. (2023). *ICMP (Internet Control Message Protocol)*. Retrieved from TechTarget: https://www.techtarget.com/searchnetworking/definition/ICMP

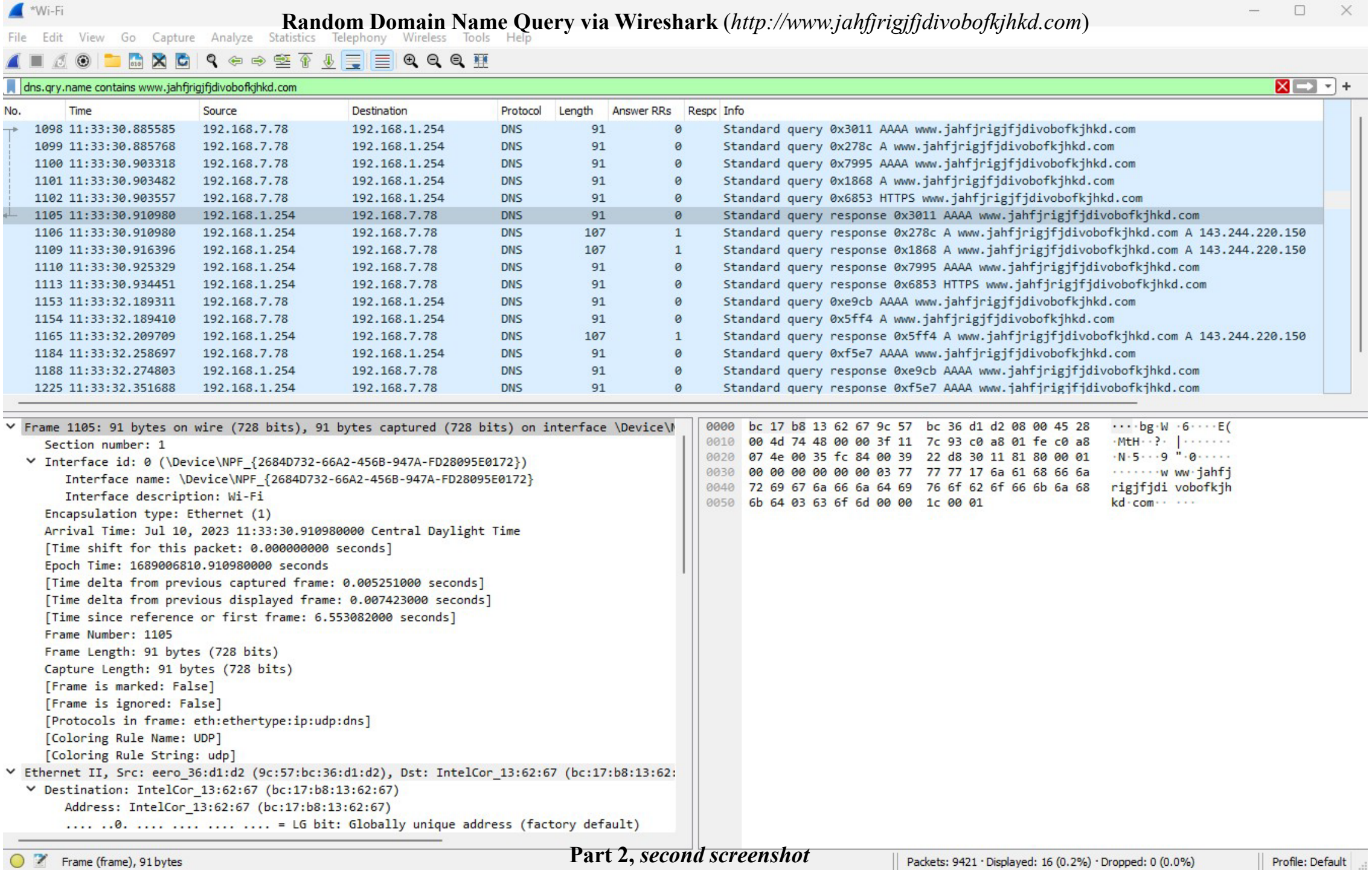
W3schools. (2023). *Wireshark Tls Client Hello Filter*. Retrieved from W3schools: https://www.w3schools.blog/wireshark-tls-client-hello-filter

DNS query via Wireshark



Part 1, *first screenshot*

Random Domain Name Query via Wireshark (*http://www.jahfjrigjfjdivobofkjhkd.com*)



Part 2, ***second screenshot***

ICMP Query via Wireshark

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpv6

No.	Time	Source	Destination	Protocol	Length	Answer RRs	Respc	Info
4458	13:30:23.967785	fe80::9e57:bcff:fe36:d1d2	2600:1700:501:338f:…	ICMPv6	86			Neighbor Solicitation for 2600:1700:501:338f:f0ed:732a:e7c4:9899 from 9
4459	13:30:23.967818	2600:1700:501:338f:f0ed:732a:e7c4:9899	fe80::9e57:bcff:fe3…	ICMPv6	86			Neighbor Advertisement 2600:1700:501:338f:f0ed:732a:e7c4:9899 (sol, ovr
4505	13:30:27.598809	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94			Echo (ping) request id=0x0001, seq=25, hop limit=128 (reply in 4506)
4506	13:30:27.624078	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94			Echo (ping) reply id=0x0001, seq=25, hop limit=56 (request in 4505)
4527	13:30:28.603481	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94			Echo (ping) request id=0x0001, seq=26, hop limit=128 (reply in 4528)
4528	13:30:28.626282	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94			Echo (ping) reply id=0x0001, seq=26, hop limit=56 (request in 4527)
4569	13:30:29.619621	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94			Echo (ping) request id=0x0001, seq=27, hop limit=128 (reply in 4570)
4570	13:30:29.647082	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94			Echo (ping) reply id=0x0001, seq=27, hop limit=56 (request in 4569)
4579	13:30:30.623553	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94			Echo (ping) request id=0x0001, seq=28, hop limit=128 (reply in 4580)
4580	13:30:30.651178	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94			Echo (ping) reply id=0x0001, seq=28, hop limit=56 (request in 4579)
8186	13:30:52.897989	fe80::ed88:583b:1487:a79	ff02::1	ICMPv6	86			Router Advertisement

```
> Frame 4527: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF
> Ethernet II, Src: IntelCor_13:62:67 (bc:17:b8:13:62:67), Dst: eero_36:d1:d2 (9c:57:bc:36:d1:d2
> Internet Protocol Version 6, Src: 2600:1700:501:338f:f0ed:732a:e7c4:9899, Dst: 2607:f8b0:4002:
> Internet Control Message Protocol v6
```

```
0000  9c 57 bc 36 d1 d2 bc 17  b8 13 62 67 86 dd 60 00   ·W·6···· ··bg··`·
0010  00 00 00 28 3a 80 26 00  17 00 05 01 33 8f f0 ed   ···(:·&· ····3···
0020  73 2a e7 c4 98 99 26 07  f8 b0 40 02 0c 09 00 00   s*····&· ··@·····
0030  00 00 00 00 00 93 80 00  0f 81 00 01 00 1a 61 62   ·····••· ·····ab
0040  63 64 65 66 67 68 69 6a  6b 6c 6d 6e 6f 70 71 72   cdefghij klmnopqr
0050  73 74 75 76 77 61 62 63  64 65 66 67 68 69         stuvwabc defghi
```

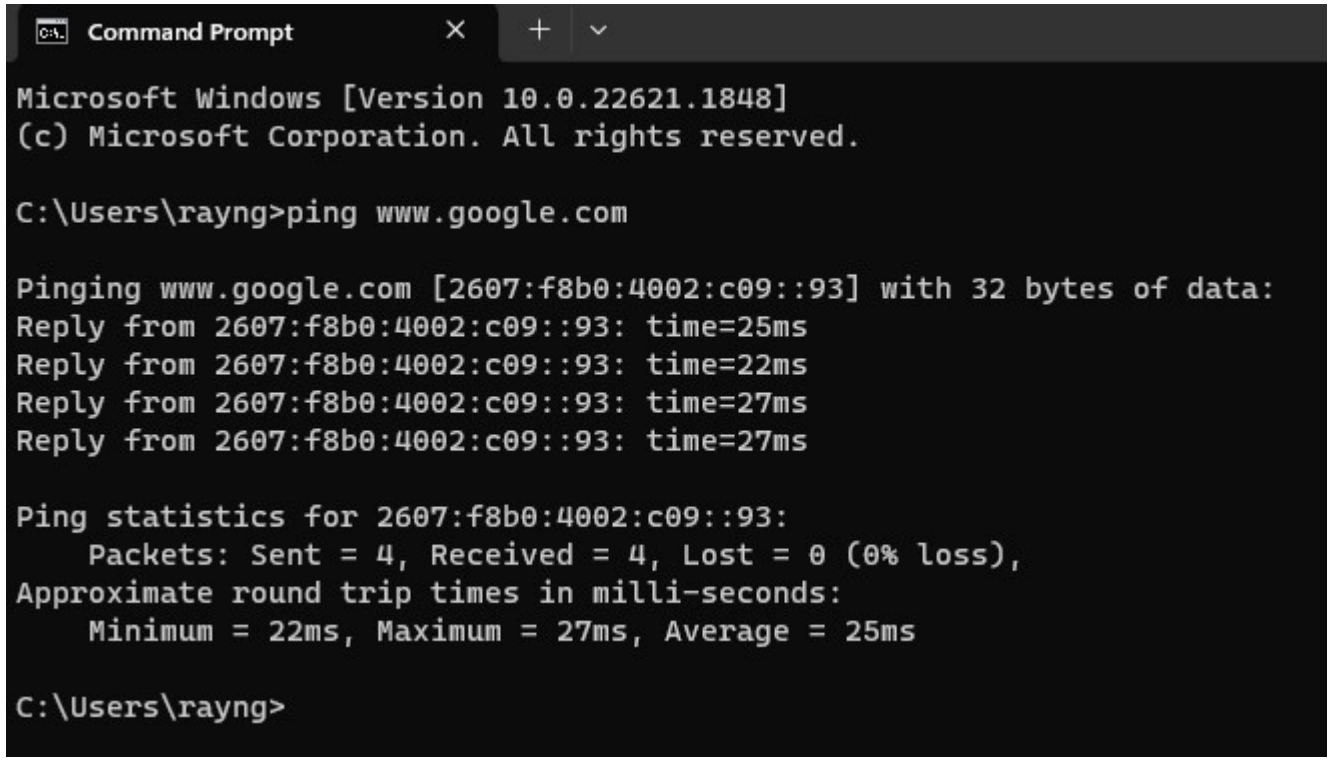
Internet Control Message Protocol v6: Protocol

Packets: 8216 · Displayed: 11 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

Part 3, *third screenshot*

ICMP Packets Containing Ping Data



4505	13:30:27.598809	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94	Echo (ping) request id=0x0001, seq=25, hop limit=128 (reply in 4506)
4506	13:30:27.624078	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94	Echo (ping) reply id=0x0001, seq=25, hop limit=56 (request in 4505)
4527	13:30:28.603481	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94	Echo (ping) request id=0x0001, seq=26, hop limit=128 (reply in 4528)
4528	13:30:28.626282	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94	Echo (ping) reply id=0x0001, seq=26, hop limit=56 (request in 4527)
4569	13:30:29.619621	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94	Echo (ping) request id=0x0001, seq=27, hop limit=128 (reply in 4570)
4570	13:30:29.647082	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94	Echo (ping) reply id=0x0001, seq=27, hop limit=56 (request in 4569)
4579	13:30:30.623553	2600:1700:501:338f:f0ed:732a:e7c4:9899	2607:f8b0:4002:c09:…	ICMPv6	94	Echo (ping) request id=0x0001, seq=28, hop limit=128 (reply in 4580)
4580	13:30:30.651178	2607:f8b0:4002:c09::93	2600:1700:501:338f:…	ICMPv6	94	Echo (ping) reply id=0x0001, seq=28, hop limit=56 (request in 4579)

Part 4, *fourth screenshot*

TLS 1.2 “Client Hello” Packet

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Destination	Protocol	Length	Answer RRs	Respc	Info
523	13:30:15.053722	192.168.7.78	13.107.5.80	TLSv1.2	571			Client Hello
535	13:30:15.066889	192.168.7.78	13.107.5.80	TLSv1.2	212			Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
536	13:30:15.067275	192.168.7.78	13.107.5.80	TLSv1.2	159			Application Data
537	13:30:15.067498	192.168.7.78	13.107.5.80	TLSv1.2	432			Application Data
551	13:30:15.079414	192.168.7.78	13.107.5.80	TLSv1.2	92			Application Data
585	13:30:15.129712	192.168.7.78	13.107.5.80	TLSv1.2	168			Application Data
6020	13:30:40.095638	192.168.7.78	13.226.204.21	TLSv1.3	571			Client Hello
6032	13:30:40.108495	192.168.7.78	13.226.204.21	TLSv1.3	118			Change Cipher Spec, Application Data
6033	13:30:40.108624	192.168.7.78	13.226.204.21	TLSv1.3	152			Application Data
6034	13:30:40.108702	192.168.7.78	13.226.204.21	TLSv1.3	459			Application Data
6042	13:30:40.113371	192.168.7.78	13.226.204.21	TLSv1.3	85			Application Data
6178	13:30:40.208973	192.168.7.78	13.86.58.123	TLSv1.3	571			Client Hello
6244	13:30:40.231814	192.168.7.78	13.86.58.123	TLSv1.3	134			Change Cipher Spec, Application Data
6245	13:30:40.232039	192.168.7.78	13.86.58.123	TLSv1.3	152			Application Data

```
    Cipher Suites Length: 32
  ▾ Cipher Suites (16 suites)
      Cipher Suite: Reserved (GREASE) (0xbaba)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
    Compression Methods Length: 1
  ▸ Compression Methods (1 method)
    Extensions Length: 403
```

```
0000  9c 57 bc 36 d1 d2 bc 17  b8 13 62 67 08 00 45 00   ·W·6···· ··bg··E·
0010  02 2d 73 a2 40 00 80 06  00 00 c0 a8 07 4e 0d 6b   ·-s·@··· ·····N·k
0020  05 50 ef 3f 01 bb 06 03  6f 74 02 82 e4 22 50 18   ·P·?···· ot···"P·
0030  02 05 dc d0 00 00 16 03  01 02 00 01 00 01 fc 03   ········ ········
0040  03 d3 91 1e 0c 27 d7 00  65 25 0c ed 06 f5 d4 8f   ·····'·· e%······
0050  f6 7d be ea f8 0e 3b 58  e8 94 04 c1 fa 62 b9 49   ·}····;X ·····b·I
0060  65 20 ca 41 24 9d b7 1c  44 d9 e9 7d 64 83 9b c5   e ·A$··· D··}d···
0070  3f 82 2c 1f 5e b2 c8 44  55 4e 61 ba cf 5a d5 74   ?·,·^··D UNa··Z·t
0080  39 d5 00 20 ba ba 13 01  13 02 13 03 c0 2b c0 2f   9·· ···· ·····+·/
0090  c0 2c c0 30 cc a9 cc a8  c0 13 c0 14 00 9c 00 9d   ·,·0···· ········
00a0  00 2f 00 35 01 00 01 93  8a 8a 00 00 00 17 00 00   ·/·5···· ········
00b0  00 10 00 0e 00 0c 02 68  32 08 68 74 74 70 2f 31   ·······h 2·http/1
00c0  2e 31 ff 01 00 01 00 00  0d 00 12 00 10 04 03 08   .1····· ········
00d0  04 04 01 05 03 08 05 05  01 08 06 06 01 00 0a 00   ········ ········
00e0  0a 00 08 da da 00 1d 00  17 00 18 00 05 00 05 01   ········ ········
00f0  00 00 00 00 00 23 00 00  00 12 00 00 00 2b 00 07   ·····#·· ·····+··
0100  06 3a 3a 03 04 03 03 44  69 00 05 00 03 02 68 32   ·::····D i·····h2
0110  00 33 00 2b 00 29 da da  00 01 00 00 1d 00 20 9e   ·3·+·)·· ······ ·
0120  75 b5 82 cb 9c 64 32 59  d8 76 9f 0a 1c 4d a5 97   u····d2Y ·v···M··
0130  ba 08 a0 be 2e 22 0f b2  e1 2a 77 60 46 8e 5d 00   ·····"·· ·*w`F·]·
0140  2d 00 02 01 01 00 0b 00  02 01 00 00 00 00 15 00   -····· ········
0150  13 00 00 10 77 77 77 2e  62 69 6e 67 61 70 69 73   ····www. bingapis
0160  2e 63 6f 6d 00 1b 00 03  02 00 02 1a 1a 00 01 00   .com···· ········
0170  00 15 00 c7 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Transport Layer Security: Protocol

Packets: 8216 · Displayed: 2053 (25.0%) · Dropped: 0 (0.0%)

Profile: Default

Part 5, *fifth screenshot*

***capture.pdf* Saved on Desktop**

"capture" file saved as .pdf
on my desktop

Part 6, *sixth screenshot*

capture.pdf **File Opened**

capture.pdf - Adobe Acrobat Pro (32-bit)

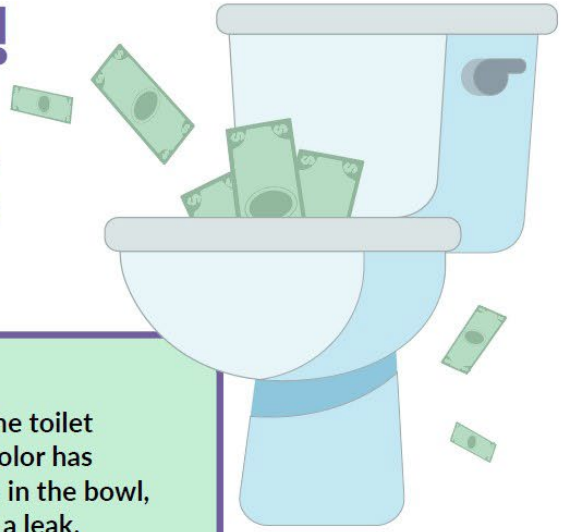
File Edit View E-Sign Window Help

Home Tools capture.pdf

STOP THAT LEAKY TOILET!

Did you know a leaky toilet can waste up to 200 gallons of water a day? That's a lot of wasted water and money flushed down the drain.

Some leaks are silent, some produce a running water sound and others may be visible as a small trickle running from the rim to the water in the bowl.



Simple steps to check for a toilet leak:

1: Start with a clean toilet free of any cleaning agents. Remove the lid to the tank.

2: Add a dye tablet, leak detector fluid or a few drops of food coloring to the tank.

3: Wait 10-15 minutes. Do not flush the toilet.

4: Look in the toilet bowl. If color has appeared in the bowl, you have a leak.

5: Flush as soon as the test is complete. Find and fix the leak or call a professional for assistance.

Southwest Florida Water Management District

Part 7, *seventh screenshot*