COMMONWEALTH OF PENNSYLVANIA
COUNTY OF LEHIGH

CIVIL COMPLAINT

Mag. Dist. No:	MDJ-31-1-01
MDJ Name:	Honorable Linda Vega Sirop
Address:	1201 Sumner Avenue Allentown, PA 18102
Telephone:	610-432-3080

PLAINTIFF: NAME and ADDRESS

HUMAN FREE WILL
617 N. LUMBER ST
ALLENTOWN, PA 18102

V.

DEFENDANT: NAME and ADDRESS

RCN
2124 AVE C
BETHLEHEM, PA

&

SERVICE ELECTRIC
2260 AVE A
BETHLEHEM, PA

	AMOUNT	DATE PAID
FILING COSTS	$ 116.25	4 / 4 / 22
POSTAGE	$ ——	/ /
SERVICE COSTS	$ 28.85	/ /
CONSTABLE ED.	$ 10.00	/ /
TOTAL	$ 155.10	/ /

Docket No: CV-54-22
Case Filed: 4/4/22

APR 04 2022

Pa.R.Civ.P.M.D.J. 206 sets forth those costs recoverable by the prevailing party.

To The Defendant: The above named plaintiff(s) asks judgment against you for $ 1776 together with costs upon the following claim (Civil fines must include citation of the statute or ordinance violated):

MY INTERNET TRAFFIC GETS ROUTED TO A PRIVATE NETWORK. IT IS NOT MY NETWORK AND IS REROUTING MY TRAFFIC AS SHOWN IN THE PROVIDED TRACES. WHAT CAN A PERSON DO TO GET OFF OF IT IF IT IS YOUR INFRASTRUCTURE?

I, MATTHEW DAY verify that the facts set forth in this complaint are true and correct to the best of my knowledge, information, and belief. This statement is made subject to the penalties of Section 4904 of the Crimes Code (18 Pa.C.S. § 4904) related to unsworn falsification to authorities.

I certify that this filing complies with the provisions of the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania that require filing confidential information and documents differently than non-confidential information and documents.

Matthew Day
(Signature of Plaintiff or Authorized Agent)

The plaintiff's attorney shall file an entry of appearance with the magisterial district court pursuant to Pa.R.Civ.P.M.D.J. 207.1.

If you intend to enter a defense to this complaint, you should notify this office immediately at the above telephone number. You must appear at the hearing and present your defense. Unless you do, judgment may be entered against you by default.

If you have a claim against the plaintiff which is within the magisterial district judge jurisdiction and which you intend to assert at the hearing, you must file it on a complaint form at this office at least five days before the date set for the hearing.

If you are disabled and require a reasonable accommodation to gain access to the Magisterial District Court and its services, please contact the Magisterial District Court at the above address or telephone number. We are unable to provide transportation.

FREE INTERPRETER
www.pacourts.us/language-rights
610-432-3080

Human Free Will is a Non Profit that helps people with technical issues. We are *Targeted Individuals* that have issues with the public infrastructure such as phone and internet service. Our mail and packages also tend to get rerouted or come days late. This is a form of covert repression.

What can we do when someone alters our communication methods?

Civil Complaint Table of Contents

V. Man in the Middle (MITM) Attacks

The private network is a form of a Man in the Middle Attack. This private network prevents us from reaching authentic websites and everything we download has malware in them. Once we connect to an untrusted network, ***everything you do on that network can be altered or restricted!***

VI. SSL Certificates Explained - google.com Example

1. The private network utilizes a DNS attack which sends you to a fake website that looks exactly like the real one. The Google search page looks very convincing until you look at the SSL cert!
2. Other sites on this private network have dead give aways but the only way to tell this Google search page has a fake SSL certificate is by looking at the short duration of the validity of the certificate. Trusted SSL certificates will have an expiration of atleast a year in duration.
3. Official SSL certificates from a reputable Certificate Authority (CA) can be costly per year.
4. Let's Encrypt is the most popular free Certificate Authority (CA).

   They only issue certificates with a max lifetime of ninety days.

VII. SSL Certificate Checker - google.com Example

The easiest way to check if an SSL Certificate is valid is to use a Certificate Checker. Since the private network utilizes a DNS attack to send you to a fake website that looks exactly like the real one, it is possible to recreate an exact copy of this site as well. The TLS Certificate is installed correctly and the chain looks valid but the certificate expiration duration is still under a year for google.com. The Issuer for the GTS Root R1 certificate is from GlobalSign Root CA and not signed by GTS Root R1. ***No average person will be able to detect this!*** I use this to compare the browser certificate with these results. Since they are different I am being rerouted somehow!

WIKIPEDIA

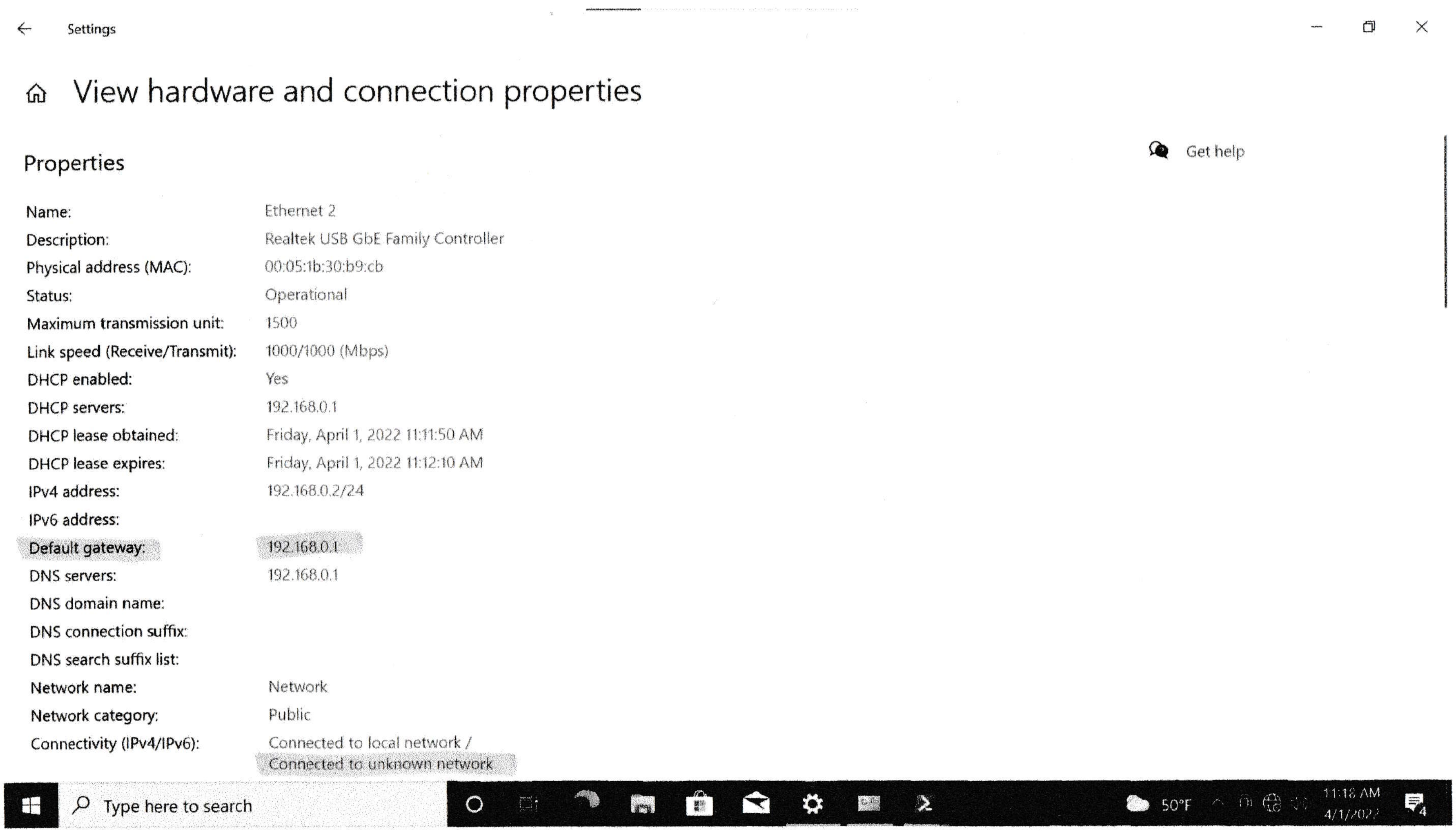
United States Declaration of Independence

United States Declaration of Independence	
United States Declaration of Independence.jpg 1823 facsimile of the engrossed copy	
Created	June–July 1776
Ratified	July 4, 1776
Location	Engrossed copy: National Archives Building Rough draft: Library of Congress
Author(s)	Thomas Jefferson, Committee of Five
Signatories	56 delegates to the Second Continental Congress
Purpose	To announce and explain separation from Great Britain[1]:5

The **United States Declaration of Independence**, formally **The unanimous Declaration of the thirteen united States of America**, is the pronouncement adopted by the Second Continental Congress meeting in Philadelphia, Pennsylvania, on July 4, 1776. Enacted during the American Revolution, the Declaration explains why the Thirteen Colonies at war with the Kingdom of Great Britain regarded themselves as thirteen independent sovereign states, no longer under British rule. With the Declaration, these new states took a collective first step in forming the United States of America. The declaration was signed by 56 of America's Founding Fathers, congressional representatives from New Hampshire, Massachusetts Bay, Rhode Island and Providence Plantations, Connecticut, New York, New Jersey, Pennsylvania, Maryland, Delaware, Virginia, North Carolina, South Carolina, and Georgia. The Declaration became one of the most circulated and widely reprinted documents in early American history.

The Lee Resolution for independence was passed by the Second Continental Congress on July 2 with no opposing votes. The Committee of Five had drafted the Declaration to be ready when Congress voted on independence. John Adams, a leader in pushing for independence, had persuaded the committee to select Thomas Jefferson to compose the original draft of the document,[2] which Congress edited to produce the final version. The Declaration was a formal explanation of why Congress had voted to declare independence from Great Britain, more than a year after the outbreak of the American Revolutionary War. Adams wrote to his wife Abigail, "The Second Day of July 1776, will be the most memorable Epocha, in the History of America";[3] although Independence Day is actually celebrated on July 4, the date that the wording of the Declaration of Independence was approved.

After ratifying the text on July 4, Congress issued the Declaration of Independence in several forms. It was initially published as the printed Dunlap broadside that was widely distributed and read to the public. The source copy used for this printing has been lost and may have been a copy in Thomas Jefferson's hand.[4] Jefferson's original draft is preserved at the Library of Congress, complete with changes made by John Adams and Benjamin Franklin, as well as Jefferson's notes of changes made by Congress. The best-known version of the Declaration is a signed copy that is displayed at the National Archives in Washington, D.C., and which is popularly regarded as the official document. This engrossed copy (finalized, calligraphic copy) was ordered by Congress on July 19 and signed primarily on August 2.[5][6]

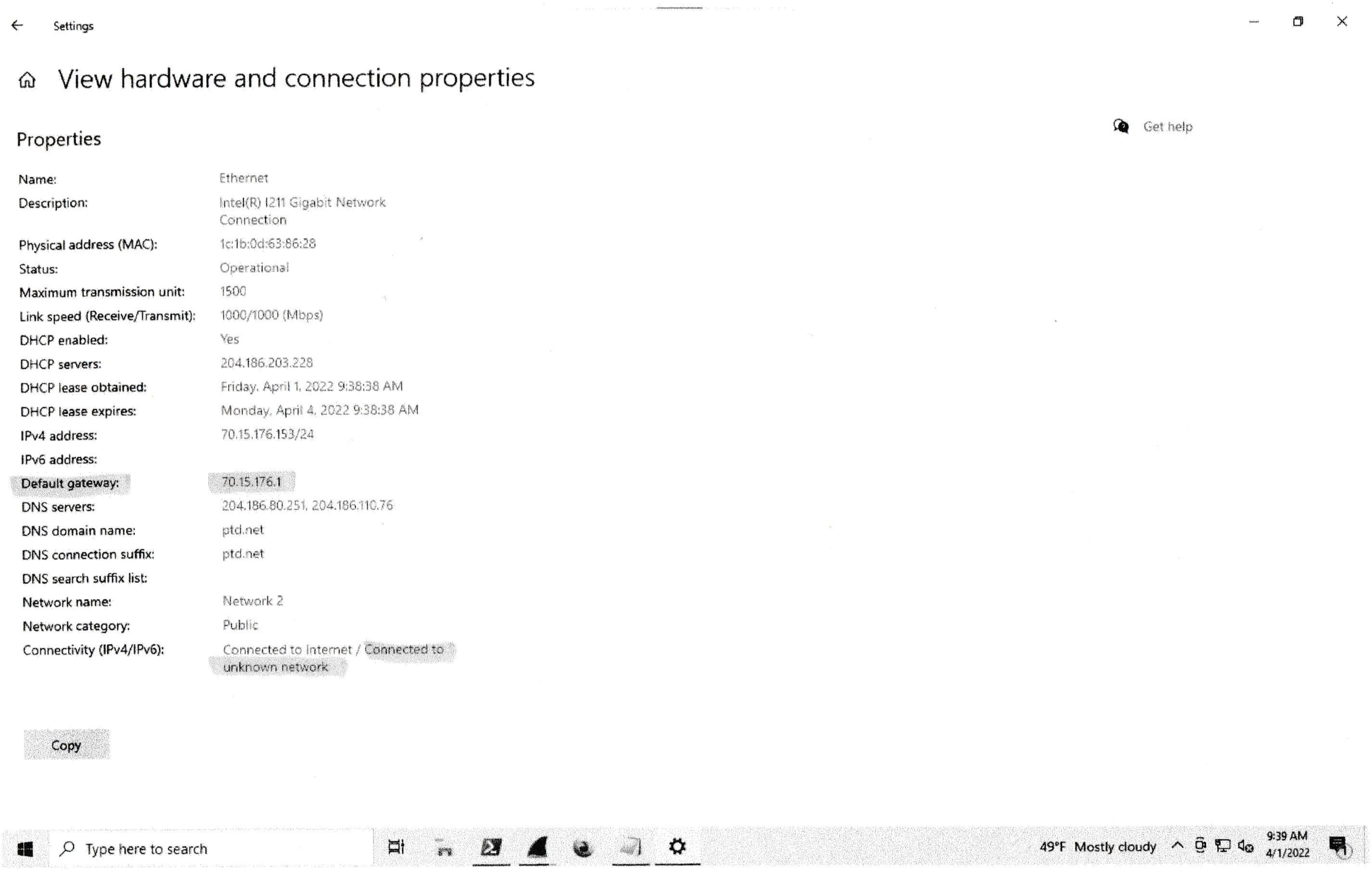


View hardware and connection properties

Properties

Name:	Ethernet 2
Description:	Realtek USB GbE Family Controller
Physical address (MAC):	00:05:1b:30:b9:cb
Status:	Operational
Maximum transmission unit:	1500
Link speed (Receive/Transmit):	1000/1000 (Mbps)
DHCP enabled:	Yes
DHCP servers:	192.168.0.1
DHCP lease obtained:	Friday, April 1, 2022 11:11:50 AM
DHCP lease expires:	Friday, April 1, 2022 11:12:10 AM
IPv4 address:	192.168.0.2/24
IPv6 address:	
Default gateway:	192.168.0.1
DNS servers:	192.168.0.1
DNS domain name:	
DNS connection suffix:	
DNS search suffix list:	
Network name:	Network
Network category:	Public
Connectivity (IPv4/IPv6):	Connected to local network / Connected to unknown network

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Matt> nslookup rcn.com
Server:  ns2.dns.rcn.net
Address:  208.59.247.45

Name:    rcn.com
Addresses:  207.172.156.181
          208.59.90.35
          207.172.156.182

PS C:\Users\Matt> tracert rcn.com

Tracing route to rcn.com [208.59.90.35]
over a maximum of 30 hops:
                                                 ROUTER
  1     3 ms    10 ms     1 ms  192.168.0.1
  2    15 ms    19 ms    27 ms  bdl1.tlg-cbr1.atw-tlg.pa.cable.rcn.net [10.50.48.1]
  3    28 ms    17 ms    22 ms  bdle8-sub211.aggr1.phdl.pa.rcn.net [207.172.196.239]
  4    21 ms    27 ms    26 ms  hge0-0-0-14.core1.phdl.pa.rcn.net [207.172.18.0]
  5    27 ms    22 ms    21 ms  207.172.19.229
  6    31 ms    26 ms    25 ms  starscream.web.rcn.net [208.59.90.35]

Trace complete.
PS C:\Users\Matt>
```



View hardware and connection properties

Properties

Name:	Ethernet
Description:	Intel(R) I211 Gigabit Network Connection
Physical address (MAC):	1c:1b:0d:63:86:28
Status:	Operational
Maximum transmission unit:	1500
Link speed (Receive/Transmit):	1000/1000 (Mbps)
DHCP enabled:	Yes
DHCP servers:	204.186.203.228
DHCP lease obtained:	Friday, April 1, 2022 9:38:38 AM
DHCP lease expires:	Monday, April 4, 2022 9:38:38 AM
IPv4 address:	70.15.176.153/24
IPv6 address:	
Default gateway:	70.15.176.1
DNS servers:	204.186.80.251, 204.186.110.76
DNS domain name:	ptd.net
DNS connection suffix:	ptd.net
DNS search suffix list:	
Network name:	Network 2
Network category:	Public
Connectivity (IPv4/IPv6):	Connected to Internet / Connected to unknown network

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Matt> nslookup sectv.com
Server:  dns.str.ptd.net
Address:  204.186.80.251

Non-authoritative answer:
Name:    sectv.com
Address:  204.186.163.245

PS C:\Users\Matt> tracert sectv.com
```

THE DEFAULT GATEWAY IS 70.15.176.1

```
Tracing route to sectv.com [204.186.163.245]
over a maximum of 30 hops:

  1     9 ms     7 ms     8 ms  10.115.196.1
  2     8 ms     6 ms     7 ms  gateway2-po4-AllBlocal1.all.ptd.net [207.44.122.21]
  3     7 ms     6 ms     7 ms  172.16.103.86
  4     8 ms     9 ms     7 ms  172.16.103.84
  5     9 ms     8 ms     8 ms  172.16.103.90
  6     *        8 ms     9 ms  172.16.103.91
  7     7 ms     7 ms     7 ms  lookup.sectv.com [204.186.163.245]
```

THIS IS ODD

```
Trace complete.
PS C:\Users\Matt> nslookup ptd.net
Server:  dns.str.ptd.net
Address:  204.186.80.251

Non-authoritative answer:
Name:    ptd.net
Address:  209.50.150.195

PS C:\Users\Matt> tracert ptd.net

Tracing route to ptd.net [209.50.150.195]
over a maximum of 30 hops:

  1     7 ms     7 ms     6 ms  10.115.196.1
  2     8 ms     6 ms     8 ms  gateway2-po4-AllBlocal1.all.ptd.net [207.44.122.21]
  3     9 ms     8 ms     9 ms  172.16.10.71
  4     9 ms    10 ms     8 ms  cpe1-pencormis.pal.ptd.net [204.186.44.132]
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Matt> nslookup sectv.com
Server:  UnKnown
Address:  10.0.1.1

Non-authoritative answer:
Name:    sectv.com
Address:  204.186.163.245

PS C:\Users\Matt> tracert sectv.com

Tracing route to sectv.com [204.186.163.245]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  APPLE [10.0.1.1]  MY ROUTER
  2    11 ms     8 ms     7 ms  10.115.196.1
  3     7 ms     8 ms     8 ms  gateway2-po4-AllBlocal1.all.ptd.net [207.44.122.21]
  4     7 ms     8 ms     9 ms  172.16.103.86
  5     9 ms     8 ms     7 ms  172.16.103.84
  6     8 ms     8 ms     8 ms  172.16.103.90
  7     9 ms     8 ms     9 ms  172.16.103.91
  8     8 ms     8 ms     7 ms  lookup.sectv.com [204.186.163.245]

Trace complete.
PS C:\Users\Matt> tracert sectv.com

Tracing route to sectv.com [204.186.163.245]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  APPLE [10.0.1.1]
  2     9 ms     8 ms     6 ms  10.115.196.1
  3     8 ms     8 ms     8 ms  gateway2-po4-AllBlocal1.all.ptd.net [207.44.122.21]
  4     8 ms     7 ms     7 ms  172.16.103.86
  5     9 ms     8 ms     7 ms  172.16.103.84
  6     8 ms     8 ms     8 ms  172.16.103.90
  7     8 ms     8 ms    10 ms  172.16.103.91
  8     8 ms     8 ms     8 ms  lookup.sectv.com [204.186.163.245]

Trace complete.
PS C:\Users\Matt> nslookup ptd.net
Server:  UnKnown
Address:  10.0.1.1

Non-authoritative answer:
Name:    ptd.net
Address:  209.50.150.195
```

```
PS C:\Users\Matt> tracert ptd.net

Tracing route to ptd.net [209.50.150.195]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  APPLE [10.0.1.1] — MY ROUTER
  2    10 ms     7 ms     7 ms  10.115.196.1
  3     8 ms     8 ms     8 ms  gateway2-po4-AllBlocal1.all.ptd.net [207.44.122.21]
  4     9 ms     9 ms     8 ms  172.16.10.65
  5    10 ms     9 ms     8 ms  cpe1-pencormis.pal.ptd.net [204.186.44.132]
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
PS C:\Users\Matt>
```

IPv4 Private Address Space and Filtering

According to standards set forth in Internet Engineering Task Force (IETF) document RFC-1918, the following IPv4 address ranges are reserved by the IANA for private internets, and are *not* publicly routable on the global internet:

- **10.0.0.0/8 IP addresses:** 10.0.0.0 – 10.255.255.255
- **172.16.0.0/12 IP addresses:** 172.16.0.0 – 172.31.255.255
- **192.168.0.0/16 IP addresses:** 192.168.0.0 – 192.168.255.255

Note that only a *portion* of the "172" and the "192" address ranges are designated for private use. The remaining addresses are considered "public," and thus are routable on the global Internet.

Use caution when setting filters to exclude these private address ranges. In some cases, Regional Internet Registries (RIRs) have issued adjacent address space to their customers and that space is in use on the global Internet.

In August 2012, ARIN began allocating "172" address space to internet service, wireless, and content providers. There have been reports from the community that many network operators are denying access to devices having IP addresses from within the entire 172 /8 range. As a result, any device with a 172.x.x.x IP address may have difficulty reaching some sites on the global Internet. The only way to solve this problem is for those operators to reconfigure their routers or firewall access controls and filter only address space from the 172.16.0.0/12 range.

≣ Rapid7 Home (https://www.rapid7.com/)

Man in the Middle (MITM) Attacks

PRODUCTS SERVICES SUPPORT & RESOURCES RESEARCH (/RESEARCH/) EN SIGN IN (HTTPS://INSIGHT.RAPID7.COM/SAML/SSO) TRY NOW

Home (/) | Fundamentals (/fundamentals/) | Man-in-the-Middle (MITM) Attacks

Man in the Middle (MITM) Attacks

MITM Techniques, Detection, and Best Practices for Prevention

What is a man-in-the-middle (MiTM) attack?

Man-in-the-middle attacks (MITM) are a common type of cybersecurity attack (/fundamentals/types-of-attacks/) that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation they should normally not be able to listen to, hence the name "man-in-the-middle."

Eve wants to eavesdrop on the conversation but also remain transparent. Eve could tell Alice that she was Bob and tell Bob that she was Alice. This would lead Alice to believe she's speaking to Bob, while actually revealing her part of the conversation to Eve. Eve could then gather information from this, alter the response, and pass the message along to Bob (who thinks he's talking to Alice). As a result, Eve is able to transparently hijack their conversation.

Types of man-in-the-middle attacks

Rogue Access Point

WIFI ATTACK

Devices equipped with wireless cards will often try to auto-connect to the access point that is emitting the strongest signal. Attackers can set up their own wireless access point and trick nearby devices to join its domain. All of the victim's network traffic can now be manipulated by the attacker. This is dangerous because the attacker does not even have to be on a trusted network to do this—the attacker simply needs a close enough physical proximity.

ARP Spoofing

THE PRIVATE NETWORK

ARP is the Address Resolution Protocol. It is used to resolve IP addresses to physical MAC (media access control) addresses in a local area network. When a host needs to talk to a host with a given IP address, it references the ARP cache to resolve the IP address to a MAC address. If the address is not known, a request is made asking for the MAC address of the device with the IP address.

An attacker wishing to pose as another host could respond to requests it should not be responding to with its own MAC address. With some precisely placed packets, an attacker can sniff the private traffic between two hosts. Valuable information can be extracted from the traffic, such as the exchange of session tokens, yielding full access to application accounts that the attacker should not be able to access.

mDNS Spoofing

Multicast DNS is similar to DNS, but it's done on a local area network (LAN) using broadcast like ARP. This makes it a perfect target for spoofing attacks. The local name resolution system is supposed to make the configuration of network devices extremely simple. Users don't have to know exactly which addresses their devices should be communicating with; they let the system resolve it for them. Devices such as TVs, printers, and entertainment systems make use of this protocol since they are typically on trusted networks. When an app needs to know the address of a certain device, such as tv.local, an attacker can easily respond to that request with fake data, instructing it to resolve to an address it has control over. Since devices keep a local cache of addresses, the victim will now see the attacker's device as trusted for a duration of time.

DNS Spoofing

Similar to the way ARP resolves IP addresses to MAC addresses on a LAN, DNS resolves domain names to IP addresses. When using a DNS spoofing attack, the attacker attempts to introduce corrupt DNS cache information to a host in an attempt to access another host using their domain name, such as www.onlinebanking.com. This leads to the victim sending sensitive information to a malicious host, with the belief they are sending information to a trusted source. An attacker who has already spoofed an IP address could have a much easier time spoofing DNS simply by resolving the address of a DNS server to the attacker's address.

Man-in-the-middle attack techniques

Sniffing

Attackers use packet capture tools to inspect packets at a low level. Using specific wireless devices that are allowed to be put into monitoring or promiscuous mode can allow an attacker to see packets that are not intended for it to see, such as packets addressed to other hosts.

Packet Injection

An attacker can also leverage their device's monitoring mode to inject malicious packets into data be part of the communication, but malicious in nature. Packet injection usually involves first sniffing to determine how and when to craft and send packets.

Session Hijacking

Most web applications use a login mechanism that generates a temporary session token to use for future requests to avoid requiring the user to type a password at every page. An attacker can sniff sensitive traffic to identify the session token for a user and use it to make requests as the user. The attacker does not need to spoof once he has a session token.

SSL Stripping

Since using HTTPS is a common safeguard against ARP or DNS spoofing, attackers use SSL stripping to intercept packets and alter their HTTPS-based address requests to go to their HTTP equivalent endpoint, forcing the host to make requests to the server unencrypted. Sensitive information can be leaked in plain text.

How to detect a man-in-the-middle attack

Detecting a Man-in-the-middle attack can be difficult without taking the proper steps. If you aren't actively searching to determine if your communications have been intercepted, a Man-in-the-middle attack can potentially go unnoticed until it's too late. Checking for proper page authentication and implementing some sort of tamper detection are typically the key methods to detect a possible attack, but these procedures might require extra forensic analysis after-the-fact.

It's important to take precautionary measures to prevent MITM attacks before they occur, rather than attempting to detect them while they are actively occurring. Being aware of your browsing practices and recognizing potentially harmful areas can be essential to maintaining a secure network. Below, we have included five of the best practices to prevent MITM attacks from compromising your communications.

Best practices to prevent man-in-the-middle attacks

Strong WEP/WAP Encryption on Access Points

Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force ☑ (/resources/testing-user-credentials-in-metasploit/) his way into a network and begin man-in-the-middle attacking. The stronger the encryption implementation, the safer.

Strong Router Login Credentials

It's essential to make sure your default router login is changed. Not just your Wi-Fi password, but your router login credentials. If an attacker finds your router login credentials, they can change your DNS servers to their malicious servers. Or even worse, infect your router with malicious software.

Virtual Private Network

VPNs can be used to create a secure environment for sensitive information within a local area network. They use key-based encryption to create a subnet for secure communication. This way, even if an attacker happens to get on a network that is shared, he will not be able to decipher the traffic in the VPN.

Force HTTPS

HTTPS can be used to securely communicate over HTTP using public-private key exchange. This prevents an attacker from having any use of the data he may be sniffing. Websites should only use HTTPS and not provide HTTP alternatives. Users can install browser plugins to enforce always using HTTPS on requests.

Public Key Pair Based Authentication

Man-in-the-middle attacks typically involve spoofing something or another. Public key pair based authentication like RSA can be used in various layers of the stack to help ensure whether the things you are communicating with are actually the things you want to be communicating with.

Google how to tell a ssl cert if valid × 🔍 ⚙ Sign in

All Videos News Images Shopping ⋮ More Tools

About 52,300,000 results (0.67 seconds)

Click the padlock icon in the address bar for the website. Click on Certificate (Valid) in the pop-up. Check the Valid from dates to validate the SSL certificate is current.

https://www.venafi.com › education-center › how-to-chec... ⋮

How To Check SSL Certificates [SSL Validation] | Venafi

About featured snippets • Feedback

https://www.keyfactor.com › how-to-check-ssl-certificate ⋮

How To Check SSL Certificates and Stay Secure - Keyfactor

To **check if SSL certificate is** installed, you can use the Certificate Manager tool and **check** its **validity** period. Another alternative option **is** to use the ...

https://support-acquia.force.com › article › 360004119... ⋮

Verifying the validity of an SSL certificate

Feb 3, 2022 — **Check** the order **of** your **certificates**: · **Verify** that the private key and main/server **certificate** match: · **Check** the dates that the **certificate is** ...

https://www.encryptionconsulting.com › education-center ⋮

What is SSL, TLS? | How to check SSL certificate Validity

How to check if an **SSL certificate is valid** · Option 1: This process **is** time-consuming. Run > certlm.msc > open Certificates Local Computer · Option 2: Download ...

https://www.howtouselinux.com › post › 4-ways-to-che... ⋮

4 Ways to Check SSL Certificate Expiration date

There are many online tools to **check** the **SSL certificate** info. https://www.digicert.com/help/ **is** one **of** them. We can input the domain name to **check** it. All the ...

https://www.sistrix.com › https-ranking-factor-update ⋮

How can I recognize a valid SSL certificate? - SISTRIX

Attention: Why a **valid SSL certificate is** important — By using an **SSL certificate** you are able to establish encrypted HTTPS connections. This **is** only ...

https://sectigostore.com › SSL Resources › Advance SSL ⋮

How Do I Know If My Site Has a Valid SSL Certificate?

How To Know If SSL Is Working? · Click on the padlock button on the address bar · Click on the "**Certificate (Valid)**" option · **Check** "**Valid** from – to" dates · Click ...

https://www.thesslstore.com › ssl-support › how-to-chec... ⋮

How to Check a Certificate's Expiration Date (Chrome)

1. Click the padlock · Click the Padlock ; 2. Click on **Valid** · **Certificate** ; 3. **Check** the Expiration Data · **Certificate** icon ; How to View your **Certificate** Expiration ...

https://learn.akamai.com › enterprise-application-access ⋮

Check the expiration date of an SSL certificate

Troubleshoot **certificate** issues by checking the expiration **of** the **certificate**.

Allentown, Pennsylvania - From your IP address - Update location

Help Send feedback Privacy Terms

Certificate

www.google.com GTS CA 1C3 GTS Root R1

Subject Name

Common Name	www.google.com

Issuer Name

Country	US
Organization	Google Trust Services LLC
Common Name	GTS CA 1C3

Validity

Not Before	Thu, 17 Mar 2022 11:49:13 GMT
Not After	Thu, 09 Jun 2022 11:49:12 GMT

Subject Alt Names

DNS Name	www.google.com

Public Key Info

Algorithm	Elliptic Curve
Key Size	256
Curve	P-256
Public Value	04:DB:DC:FB:11:9F:0A:EA:1B:E4:F2:F3:C3:42:B7:A7:56:DA:96:07:55:A1:D...

Miscellaneous

Renew your plan and reissue your certificate in 1 year.

Already a DigiCert customer? Sign in

Step 1
Configure your certificate

Step 2
Add account and organization details

Step 3
Check out

Your DigiCert certificate

Secure Site SSL

- All features in Basic OV
- Supports single domain, subject alternative names (SANs), and wildcard domains
- Priority validation and support for prompt issuance and service
- Premium site seals to show proof of trust
- Malware checking to protect your site availability and online revenue

> Choose a different product | Compare TLS/SSL products

1. Choose your multi-year plan

1 year plan

2. Enter your website and server information

I don't have my CSR [redacted]

Add your CSR ⓘ

Need help with your CSR?

Upload your CSR or paste it here

For compliance and security, generate your CSR with a 2048-bit or greater key pair.

Server app details for the host you install the certificate on

Apache

Your main website URL (www.mydomain.com) or wildcard domain (*.mydomain.com)

Additional standard or wildcard URLs to secure with subject alternative names (SANs) (optional)
Separate SANs with commas or line breaks

Order summary

Secure Site SSL

1-year plan

Price details

Base price Primary URL x 1 year	$448.00 USD
Subtotal	$448.00 USD
Total	$448.00 USD Applicable tax not included

Terms of use Privacy policy Legal repository Webtrust audits

DigiCert.com

Secure checkout

Let's Encrypt

Documentation Get Help Donate ▾ About Us ▾ Languages ▾

About Let's Encrypt

Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG).

We give people the digital certificates they need in order to enable HTTPS (SSL/TLS) for websites, for free, in the most user-friendly way we can. We do this because we want to create a more secure and privacy-respecting Web.

You can read about our most recent year in review by downloading our annual report.

The key principles behind Let's Encrypt are:

- **Free:** Anyone who owns a domain name can use Let's Encrypt to obtain a trusted certificate at zero cost.
- **Automatic:** Software running on a web server can interact with Let's Encrypt to painlessly obtain a certificate, securely configure it for use, and automatically take care of renewal.
- **Secure:** Let's Encrypt will serve as a platform for advancing TLS security best practices, both on the CA side and by helping site operators properly secure their servers.
- **Transparent:** All certificates issued or revoked will be publicly recorded and available for anyone to inspect.
- **Open:** The automatic issuance and renewal protocol is published as an open standard that others can adopt.
- **Cooperative:** Much like the underlying Internet protocols themselves, Let's Encrypt is a joint effort to benefit the community, beyond the control of any one organization.

Let's Encrypt

Documentation Get Help Donate ▾ About Us ▾ Languages ▾

Why ninety-day lifetimes for certificates?

Nov 9, 2015 • Josh Aas, ISRG Executive Director

We're sometimes asked why we only offer certificates with ninety-day lifetimes. People who ask this are usually concerned that ninety days is too short and wish we would offer certificates lasting a year or more, like some other CAs do.

Ninety days is nothing new on the Web. According to Firefox Telemetry, 29% of TLS transactions use ninety-day certificates. That's more than any other lifetime. From our perspective, there are two primary advantages to such short certificate lifetimes:

1. They limit damage from key compromise and mis-issuance. Stolen keys and mis-issued certificates are valid for a shorter period of time.
2. They encourage automation, which is absolutely essential for ease-of-use. If we're going to move the entire Web to HTTPS, we can't continue to expect system administrators to manually handle renewals. Once issuance and renewal are automated, shorter lifetimes won't be any less convenient than longer ones.

For these reasons, we do not offer certificates with lifetimes longer than ninety days. We realize that our service is young, and that automation is new to many subscribers, so we chose a lifetime that allows plenty of time for manual renewal if necessary. We recommend that subscribers renew every sixty days. Once automated renewal tools are widely deployed and working well, we may consider even shorter lifetimes.

Support a more secure and privacy-respecting Web.

digicert (/) **TLS/SSLPKIIoTSolutionsAboutSupport**

DigiCert® SSL Installation Diagnostics Tool

SSL Certificate Checker

LIVE CHAT

If you are having a problem with your SSL certificate installation, please enter the name of your server. Our installation diagnostics tool will help you locate the problem and verify your SSL Certificate installation.

Get Help Now!

Click here for live help with your SSL installation.

Server Address: *(Ex. www.digicert.com)*

google.com

CHAT NOW >

□**Check for common vulnerabilities**

CHECK SERVER

DNS resolves google.com to 172.217.5.110

HTTP Server Header: gws

The Certificate is not issued by DigiCert, GeoTrust, Thawte, or RapidSSL

Make sure the website you want to check is secured by a certificate from one of our product lines.

```
Common Name = *.google.com
Subject Alternative Names = *.google.com, *.appengine.google.com, *.bdn.dev,
  *.cloud.google.com, *.crowdsource.google.com, *.datacompute.google.com,
  *.google.ca, *.google.cl, *.google.co.in, *.google.co.jp, *.google.co.uk,
  *.google.com.ar, *.google.com.au, *.google.com.br, *.google.com.co,
  *.google.com.mx, *.google.com.tr, *.google.com.vn, *.google.de, *.google.es,
  *.google.fr, *.google.hu, *.google.it, *.google.nl, *.google.pl, *.google.pt,
  *.googleadapis.com, *.googleapis.cn, *.googlevideo.com, *.gstatic.cn,
  *.gstatic-cn.com, googlecnapps.cn, *.googlecnapps.cn, googleapps-cn.com,
  *.googleapps-cn.com, gkecnapps.cn, *.gkecnapps.cn, googledownloads.cn,
  *.googledownloads.cn, recaptcha.net.cn, *.recaptcha.net.cn, recaptcha-cn.net,
  *.recaptcha-cn.net, widevine.cn, *.widevine.cn, ampproject.org.cn,
  *.ampproject.org.cn, ampproject.net.cn, *.ampproject.net.cn, google-analytics-
  cn.com, *.google-analytics-cn.com, googleadservices-cn.com, *.googleadservices-
  cn.com, googlevads-cn.com, *.googlevads-cn.com, googleapis-cn.com,
  *.googleapis-cn.com, googleoptimize-cn.com, *.googleoptimize-cn.com,
  doubleclick-cn.net, *.doubleclick-cn.net, *.fls.doubleclick-cn.net,
  *.g.doubleclick-cn.net, doubleclick.cn, *.doubleclick.cn, *.fls.doubleclick.cn,
  *.g.doubleclick.cn, dartsearch-cn.net, *.dartsearch-cn.net,
  googletraveladservices-cn.com, *.googletraveladservices-cn.com,
  googletagservices-cn.com, *.googletagservices-cn.com, googletagmanager-cn.com,
  *.googletagmanager-cn.com, googlesyndication-cn.com, *.googlesyndication-
  cn.com, *.safeframe.googlesyndication-cn.com, app-measurement-cn.com, *.app-
  measurement-cn.com, gvt1-cn.com, *.gvt1-cn.com, gvt2-cn.com, *.gvt2-cn.com,
  2mdn-cn.net, *.2mdn-cn.net, googleflights-cn.net, *.googleflights-cn.net,
  admob-cn.com, *.admob-cn.com, *.gstatic.com, *.metric.gstatic.com, *.gvt1.com,
  *.gcpcdn.gvt1.com, *.gvt2.com, *.gcp.gvt2.com, *.url.google.com, *.youtube-
  nocookie.com, *.ytimg.com, android.com, *.android.com, *.flash.android.com,
  g.cn, *.g.cn, g.co, *.g.co, goo.gl, www.goo.gl, google-analytics.com, *.google-
  analytics.com, google.com, googlecommerce.com, *.googlecommerce.com, ggpht.cn,
  *.ggpht.cn, urchin.com, *.urchin.com, youtu.be, youtube.com, *.youtube.com,
  youtubeeducation.com, *.youtubeeducation.com, youtubekids.com,
  *.youtubekids.com, yt.be, *.yt.be, android.clients.google.com,
  developer.android.google.cn, developers.android.google.cn,
  source.android.google.cn
Issuer = GTS CA 1C3
Serial Number = DA5C24AAEE3D19981200000000005A61D
SHA1 Thumbprint = 9A71DEE71AB225CAB4F23649ABCEF6256204E43C
Key Length = 256
Signature algorithm = SHA256-RSA
Secure Renegotiation:
```

digicert (/) TLS/SSL PKI IoT Solutions About Support

TLS Certificate has not been revoked

OCSP Staple: Not Enabled

OCSP Origin: Good

CRL Status: Good

TLS Certificate expiration

The certificate expires June 9, 2022 (70 days from today)

Certificate Name matches google.com

SERVER CERTIFICATE

Subject *.google.com

Valid from 17/Mar/2022 to 09/Jun/2022

Issuer GTS CA 1C3

INTERMEDIATE CERTIFICATE

Subject GTS CA 1C3

Valid from 13/Aug/2020 to 30/Sep/2027

Issuer GTS Root R1

INTERMEDIATE CERTIFICATE

Subject GTS Root R1

Valid from 19/Jun/2020 to 28/Jan/2028

Issuer GlobalSign Root CA

TLS Certificate is correctly installed

Congratulations! This certificate is correctly installed.

Helpful SSL Tools

- Discovery (https://docs.digicert.com/certificate-tools/discovery-user-guide/) - Discover and analyze every certificate in your enterprise.
- DigiCert Certificate Utility for Windows (https://www.digicert.com/util/) – Simplifies SSL and code signing certificate management and use.
- Exchange 2007 (https://www.digicert.com/easy-csr/exchange2007.htm) / Exchange 2010 CSR Wizard (https://www.digicert.com/easy-csr/exchange2010.htm) - Exchange administrators love our Exchange CSR Wizards. They help you create a New-ExchangeCertificate command without having to dig through a manual.