Overview of DNS

Charles S. Givre CISSP

Overview

- What is DNS?
- How does it work?
- How can you gather DNS data for analytics?
- What can you learn from DNS analytics?

What is DNS?

- DNS stands for **D**omain **N**ame **S**ystem and can be thought of as a phonebook for the internet.
- DNS servers translate domain names into resolvable IP addresses which can be used to retrieve information from remote servers.
- This allows us to use human-readable names instead of IP addresses to access websites and other resources.
- DNS requests are sent over port 53.

DNS Terms

- **Domain Name Service** (DNS) resolves domain names to IP addresses (like a phone book)
- **Domain Registrars**: authority that signs unique domain names (GoDaddy, BlueGator)
- **State of Authority** (SOA): Contains for example name of server for zone, administrator of zone, default time-to-live (ttl = time a DNS record is cached), seconds of secondary name server should wait before checking for updates
- **Root Zone** controlled by Internet Assigned Numbers Authority (IANA)
- **Name Servers** (NS Records): used by tld servers to direct traffic to DNS server (which contains authoritative DNS records)
- **A records** (part of DNS record): "A" stands for IP Address
- **CNAME** (part of DNS record): resolves one domain name to another
- **Autonomous System** (AS) and Border gateway Protocol (BGP) info

Python libraries: `python-whois, dnspython, tldextract, ipaddress`

DNS Server Types

- **DNS Recursor:** The "librarian" who finds a book in a library. The recursor will make multiple queries until the resolution is completed.
- **Root Nameserver:** The root name server is the first step in DNS resolution. Usually it serves as a reference to other locations.
- **TLD Nameserver:** The Top Level Domain(TLD) contains DNS records for the last portion of a hostname. TLDs are .com, .org, .ca etc.
- **Authoritative Nameserver:** The final name server which contains records for the initial request.

List of Root Servers

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

https://www.iana.org/domains/root/servers

DNS Resolution

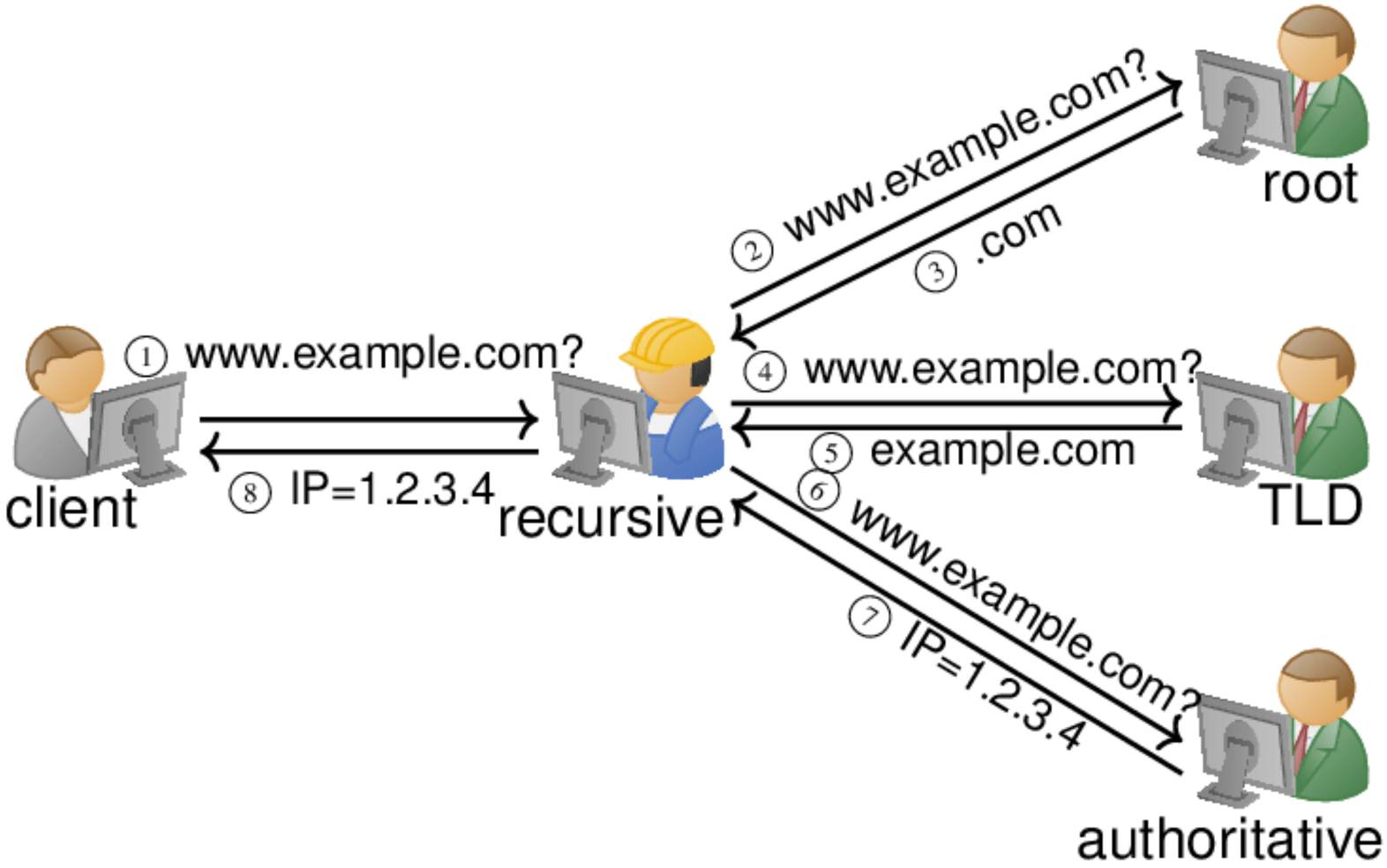
The basic process of a DNS resolution follows these steps:

1. The user enters a web address or domain name into a browser.
2. The browser sends a message, called a ***recursive DNS query***, to the network to find out which IP or network address the domain corresponds to.
3. The query goes to a ***recursive DNS server***, which is also called a recursive resolver, and is usually managed by the internet service provider (ISP). If the recursive resolver has the address, it will return the address to the user, and the webpage will load.
4. If the recursive DNS server does not have an answer, it will query a series of other servers in the following order: DNS root name servers, ***top-level domain*** (TLD) name servers and authoritative name servers.
5. The three server types work together and continue redirecting until they retrieve a DNS record that contains the queried IP address. It sends this information to the recursive DNS server, and the webpage the user is looking for loads. DNS root name servers and TLD servers primarily redirect queries and rarely provide the resolution themselves.
6. The recursive server stores, or caches, the **A record** for the domain name, which contains the IP address. The next time it receives a request for that domain name, it can respond directly to the user instead of querying other servers.
7. If the query reaches the ***authoritative server*** and it cannot find the information, it returns an error message.

The entire process querying the various servers takes a fraction of a second and is usually imperceptible to the user.

https://www.techtarget.com/searchnetworking/definition/domain-name-system

DNS Flow


root
② www.example.com?
③ .com
client
① www.example.com?
⑧ IP=1.2.3.4
recursive
④ www.example.com?
⑤ example.com
TLD
⑥ www.example.com?
⑦ IP=1.2.3.4
authoritative

What does a DNS record look like?

```
dig <domain>

# To check on a specific server
dig @dns.server.name.or.ip domain.name
```

Other DNS Tools

- nslookup
- host

DNS Records (Zone Files)

What's in a DNS Record?

- **A record**: Contains the IPv4 address associated with a domain
- **AAAA record**: Contains the IPv6 address associated with a domain.
- **CNAME record**: Forwards a subdomain to another domain
- **MX record**: Directs mail to an email server
- **NS record**: Stores the name server entries for a DNS entry
- **PTR Record**: Provides information for reverse lookups.
- **SOA record**: Administration information about a domain.
- **TXT Record:** Contains text parameters such as validators.

What does a DNS record look like?

```
; <<>> DiG 9.10.6 <<>> crtc.gc.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28572
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;crtc.gc.ca.                            IN        A

;; ANSWER SECTION:
crtc.gc.ca.                 1          IN        A          198.103.61.7

;; Query time: 25 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Mar 19 12:30:43 EDT 2023
;; MSG SIZE  rcvd: 55
```

DNS Response

Record	Type	Value	TTL
gtkcyber.com	A	35.224.172.16	3600
gtkcyber.com	MX	5 alt1.aspmx.l.google.com.	3600
gtkcyber.com	MX	10 alt3.aspmx.l.google.com.	3600
gtkcyber.com	MX	1 aspmx.l.google.com.	3600
gtkcyber.com	MX	10 alt4.aspmx.l.google.com.	3600
gtkcyber.com	MX	5 alt2.aspmx.l.google.com.	3600
gtkcyber.com	NS	ns-cloud-b4.googledomains.com.	21600
gtkcyber.com	NS	ns-cloud-b1.googledomains.com.	21600
gtkcyber.com	SOA	ns-cloud-b1.googledomains.com. cloud-dns-hostmaster.google.com. 47 21600 3600 259200 300	21600
gtkcyber.com	TXT	"v=spf1 include:_spf.google.com ~all"	3600

DNS Caching

- Due to the speed required and low frequency of changes, DNS information is cached extensively.
- DNS information is cached in most modern browsers
- DNS information is also cached in a file known as the *hosts* file on a local machine.

DNS Cache Poisoning

- DNS Cache Poisoning is a type of MITM attack whereby a victim computer receives a forged DNS response, thereby redirecting web traffic to a site(s) controlled by an attacker.
- Malware can also remove entries in a victim's host file to prevent the victim from accessing antivirus software or for other malicious purposes.
- DNS Cache Poisoning is possible because DNS requests are made over UDP and there is no verification for DNS requests.

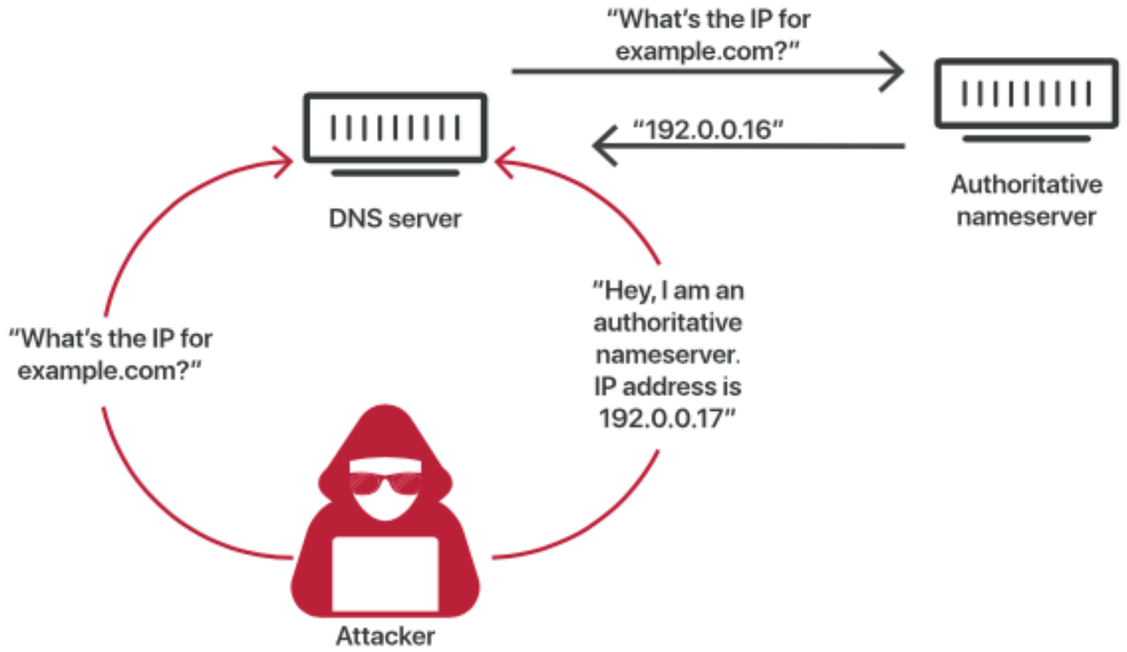


Diagram Credit: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

What can you learn from DNS?
DNS Reconnaissance

What can you learn from DNS?

- A LOT!!
- Improperly configured DNS can reveal non-public subdomains and other potentially sensitive server information.
- DNS can reveal services used by the parent organization.
- DNS information can reveal non-public administration information.

TXT Messages

Apache Drill Query Profiles Storage Metrics Threads Logs

Query Profile: 1be6da5b-7053-4aea-6708-9a348c41bf94 COMPLETED

Column visibility Show 25 entries

name	type	rdata
takeaway.com.	TXT	"1password-site-verification=BIR4NNXSUREIBHFKAXPZM67PSA"
takeaway.com.	TXT	"553489244-2954179"
takeaway.com.	TXT	"apple-domain-verification=W3pQJi76x3dq95qs"
takeaway.com.	TXT	"ca3-81d1f62392674a59abff7b00fef335c5"
takeaway.com.	TXT	"google-site-verification=2FdELXbyXygBbiv0gCC6g0t50gnMOdgpyD6tOkL2XUI"
takeaway.com.	TXT	"google-site-verification=4JZfetImPNuWS_vFNjM82Kug3FonxSbU5fXszb9cNqg"
takeaway.com.	TXT	"google-site-verification=AKDOQuZDq-XksrC9nYuem6mzuRvfpCr2OZvREbUn5G4"
takeaway.com.	TXT	"google-site-verification=J7WyVluYRLo8269AZbjV9vzkE73EGebeU9aopWoou1U"
takeaway.com.	TXT	"google-site-verification=OeatN3JYAY03JlITgXCTX7f_V0JdbTpx9ClUl9oPd6o"
takeaway.com.	TXT	"google-site-verification=bqCJa20OuYhY52EtAUeTJGiqqMxQfPa0zg1odHm5W78"
takeaway.com.	TXT	"google-site-verification=doexddN4NhpHhk8JTXJydLdufCQkDkUQLKmctCSYJNE"
takeaway.com.	TXT	"google-site-verification=gSu4gdGGeLDOZpWaVWNWYrMUxgKHEeb-pAVSm542kWU"
takeaway.com.	TXT	"v=spf1 include:_spf.takeaway.com -all"
takeaway.com.	TXT	"zapier-domain-verification-challenge=156ab3b7-67a9-43a4-9416-5b2dfd934d96"

Zone Transfers

- A zone transfer is when a DNS Server sends a domain's entire zone file to an unauthenticated user.
- Occurs when a DNS server responds to a global Asynchronous Transfer Full Range (AXFR) request.
- Can reveal internal network structure, subdomains and other non-public information about an organization.
- The "easy" solution to preventing a zone transfer is configuring your DNS to only allow AXFR requests from known IP addresses.

DSN vs. Whois

- DNS records information linking domain names with IP addresses
- Whois records are maintained by registrars and contain administrative information about domains.
- To register a domain, an organization must provide a billing, administrative and technical contact. These can be the same individual.

WHOIS Example

```
organisation: Canadian Internet Registration Authority
(CIRA) Autorité Canadienne pour les enregistrements Internet
(ACEI)
address:      979 Bank Street, Suite 400
address:      Ottawa ON K1S 5K5
address:      Canada

contact:      administrative
name:         Chief Information Officer
organisation: CIRA
address:      979 Bank Street, Suite 400
address:      Ottawa ON K1S 5K5
address:      Canada
phone:        +1 613 237 5335
fax-no:       +1 613 237 0534
e-mail:       chief.information.officer@cira.ca
```

WHOIS Example

```
contact:      technical
name:         DNS Admin
organisation: CIRA
address:      979 Bank Street, Suite 400
address:      Ottawa ON K1S 5K5
address:      Canada
phone:        +1 613 237 5335
fax-no:       +1 613 237 0534
e-mail:       admin-dns@cira.ca


nserver:      ANY.CA-SERVERS.CA 199.4.144.2
2001:500:a7:0:0:0:0:2
nserver:      C.CA-SERVERS.CA 185.159.196.2
2620:10a:8053:0:0:0:0:2
nserver:      J.CA-SERVERS.CA 198.182.167.1
2001:500:83:0:0:0:0:1
nserver:      X.CA-SERVERS.CA 199.253.250.68
```

Domain Hijacking

- Domain hijacking can occur when an unauthorized actor takes control of a victim's domain.
- This can happen if a name server is compromised, social engineering to access registrar information or from other tactics.
- If a malicious actor gains control of your zone, they can create unauthorized subdomains, redirect traffic to malicious impersonation sites.

Preventing Domain Hijacking

- Registrars can lock domains the prevent unauthorized changes.
- This would be reflected in the whois record. You will see something like: *Registrar Lock* or *Client Transfer Prohibited* in the record.
- Domain privacy services also exist to conceal contact information in domain registrations. This can prevent spoofing.

Securing DNS

- DNS in its original implementation is not a secure protocol. DNS does not validate the authenticity of the responses and as such it is possible for a malicious actor to reroute traffic through malicious servers.
- DNSSEC adds cryptographic signatures to DNS records to ensure the authenticity of DNS requests.

Other DNS Mischief

- DOS/DDoS Attacks:
- DNS Amplification Attacks
- Pattern of Life Analysis

Securing Email

MX Records

- MX (**m**ail e**x**change) records directs email to a mail server.
- MX records must point to another domain, as a CNAME record.
- MX records contain a priority which indicates the preference for which server to access first.

crtc.gc.ca	record type:	priority	value	TTL
@	MX	10	mailhost1.crtc.gc.ca	45000
@	MX	20	mailhost2.crtc.gc.ca	45000

Securing Email

- The standard email protocols were not originally designed for security and thus have many holes in them which permit spoofing and other malicious activity.
- Additionally, since emails pass through many servers en-route to their destination, it is entirely possible for a malicious email server to modify messages in transit.

Securing Email

In response to these challenges, several protocols were developed to make email-based attacks more difficult. Each serves a different purpose. They are:

- Secure Policy Framework (SPF): Restricts who can send email from a domain.
- Domain Keys Identified Mail (DKIM): Ensures that the content of email remains trusted.
- Domain-based Message Authentication, Reporting and Conformance (DMARC): Verifies alignment between from domain and SPF and DKIM authentication.

Securing Email

- In October 2017, the US Government issued Binding Operational Directive 18-01 Enhancing Email and Web Security mandating the use of SPF, DKIM and DMARC on government email.
- Canadian Government also requires the use of SPF, DKIM and DMARC on all government email. (https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/email.html)

Secure Policy Framework (SPF)

- SPF is a means of restricting who can send emails from a given domain.
- SPF is implemented by adding a specially formatted TXT record to your zone file.
- When an email is received, the receiver email server will use the DNS information, combined with information in the email header to determine whether the email is valid or not.

SPF: How it Works

- Outgoing email must have a `return-path` address included in email header.
- Upon receipt, the `return-path` domain is extracted and the mail server pull the DNS record for that domain.
- The recipient email server then verifies that the IP address associated with the return-path domain is in the SPF record.
- If not, the email is treated as spam.
- Note: The `return-path` domain does not have to match the `From:` domain.

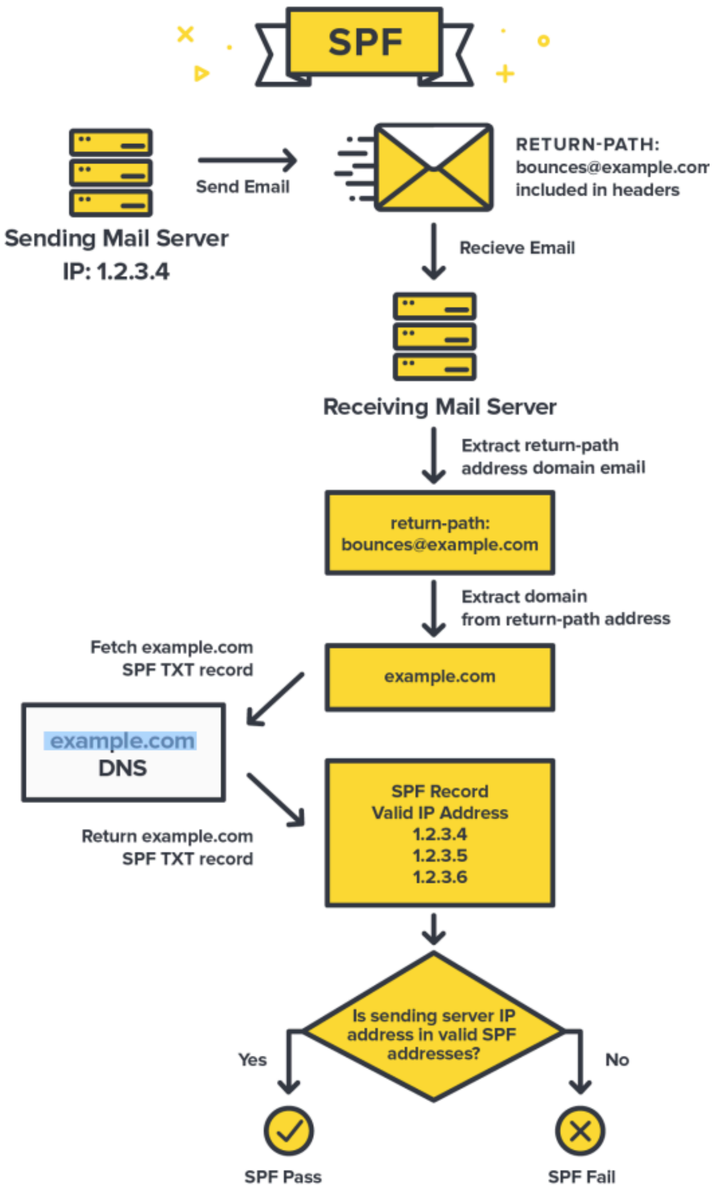


Diagram Credit: https://postmarkapp.com/guides/spf

SPF Record Syntax

name	type	rdata
crtc.gc.ca.	TXT	"1nVRxoybhG36k3kAC1lhqAmEOEwUlq4tXoFL0f2cr/FCt9YpySJXGQvFobmBrNTfgg+nRXoGSluKJcZByQSRlQ=="
crtc.gc.ca.	TXT	"apple-domain-verification=bgkYe4UjzMc2nSxS"
crtc.gc.ca.	TXT	"MS=95E8C17FEF3155E5CCDBF14D0049986F28989E1F"
crtc.gc.ca.	TXT	"MS=4B663D8CFAB79D3274AD9F17A827972A84D04C28"
crtc.gc.ca.	TXT	"MS=ms65573337"
crtc.gc.ca.	TXT	"v=spf1 mx a ip4:198.103.61.0/24 include:spf.protection.outlook.com include:spf.cyberimpact.com ~all"
crtc.gc.ca.	TXT	"cisco-ci-domain-verification=4ab9438702cb30f1a63bbad1bf28dabf488b6e842359a71a264bb4f768e4a8e2"

Showing 1 to 7 of 7 entries

Previous 1 Next

SPF Record Syntax

```
v=spf1 a mx include:example.com ~all
```

`v=spf1`: This is the SPF version being used.

`a`: This mechanism requires that the IP address of the sending domain has an A record that matches the mail server IP.

`mx`: This mechanism specifies which email servers can relay email.

`~all`: Allows anything else to soft fail

Modifiers

+	Pass
-	Fail
~	Soft Fail
?	Neutral

DomainKeys Identified Mail (DKIM)

- DKIM involves the cryptographic signing of individual email messages.
- DKIM does NOT encrypt the actual contents of the email.
- The receiver authenticates DKIM-signed email by using the public key posted at the domain from the DKIM header. The receiver will compare the signature in the email header with one it calculates. If the signatures match, the email is considered legitimate.

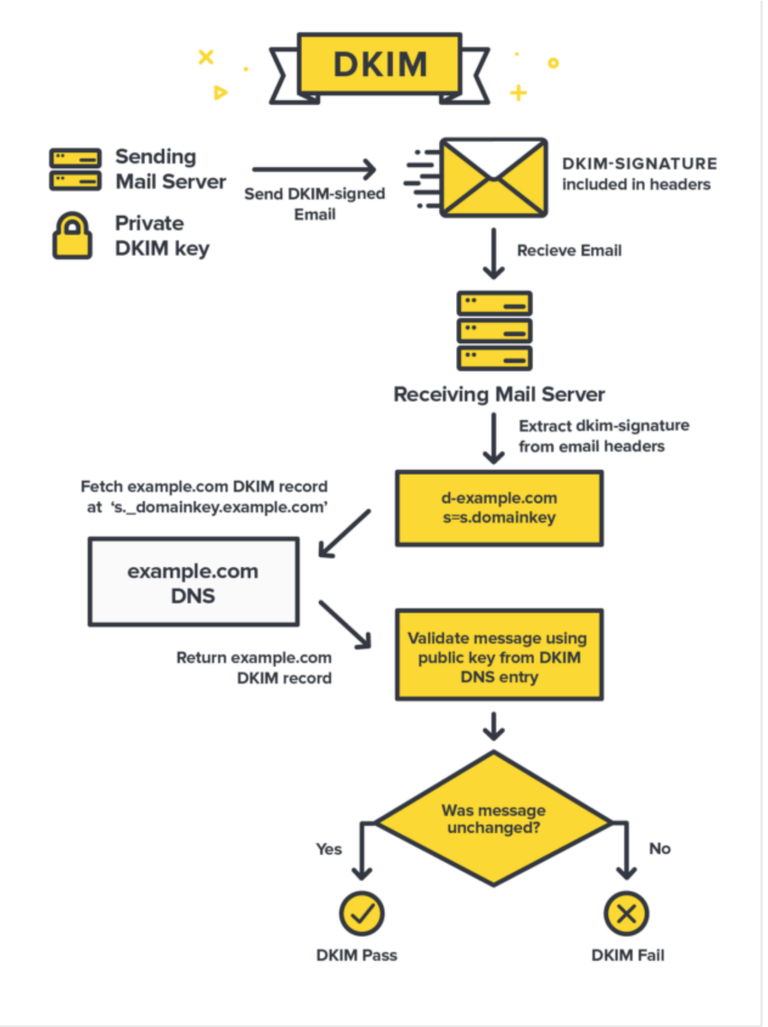


Diagram Credit: https://postmarkapp.com/guides/dkim/how-does-dkim-work

DomainKeys Identified Mail (DKIM)

- DKIM is set up by using a TXT or CNAME record in your DNS Zone.

```
k=rsa; t=s;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGMjj8MVaESl30KSPYdLaEreSYzvOVh15u9YKA
mTLgk1ecr4BCRq3Vkg3Xa2QrEQWbIvQj9FNqBYOr3XIczzU8gkK5Kh42P4C3DgNiBvlNNk2BlA5ITN
/EvVAn/ImjoGq5IrcO+hAj2iSAozYTEpJAKe0NTrj49CIkj5JI6ibyJwIDAQAB
```

- k is the algorithm, p is the public key.
- The name in the Zone file is known as a selector prefix and should be unique from all other keys in the zone file.

DomainKeys Identified Mail (DKIM)

The header to the right is what gets inserted into an email.

- v is the version of DKIM
- a=rsa-sha1: The algorithm used to generate the keys
- d: The domain used to generate the keys
- b: The generated signature
- bh: The value body of a body hash before the message headers are signed.

```
DKIM-Signature a=rs-sha1; q=dns;
      d=example.com;
      i=user@eng.example.com;
      s=jun2005.eng; c=relaxed/simple;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
      av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```


https://www.sonicwall.com/support/knowledge-base/what-is-dkim-record-and-how-to-create-it/170504710515852/

DomainKeys Identified Mail (DKIM)

- To verify a DKIM record, use the following command.

```
dig +short google._domainkey.example.com TXT
```

Try it yourself!

Questions?

DMARC

- DMARC works on top of SPF and DKIM.
- DMARC policies are set in your DNS Zone File.
- In addition, DMARC can generate reporting about sending activity on your domain.

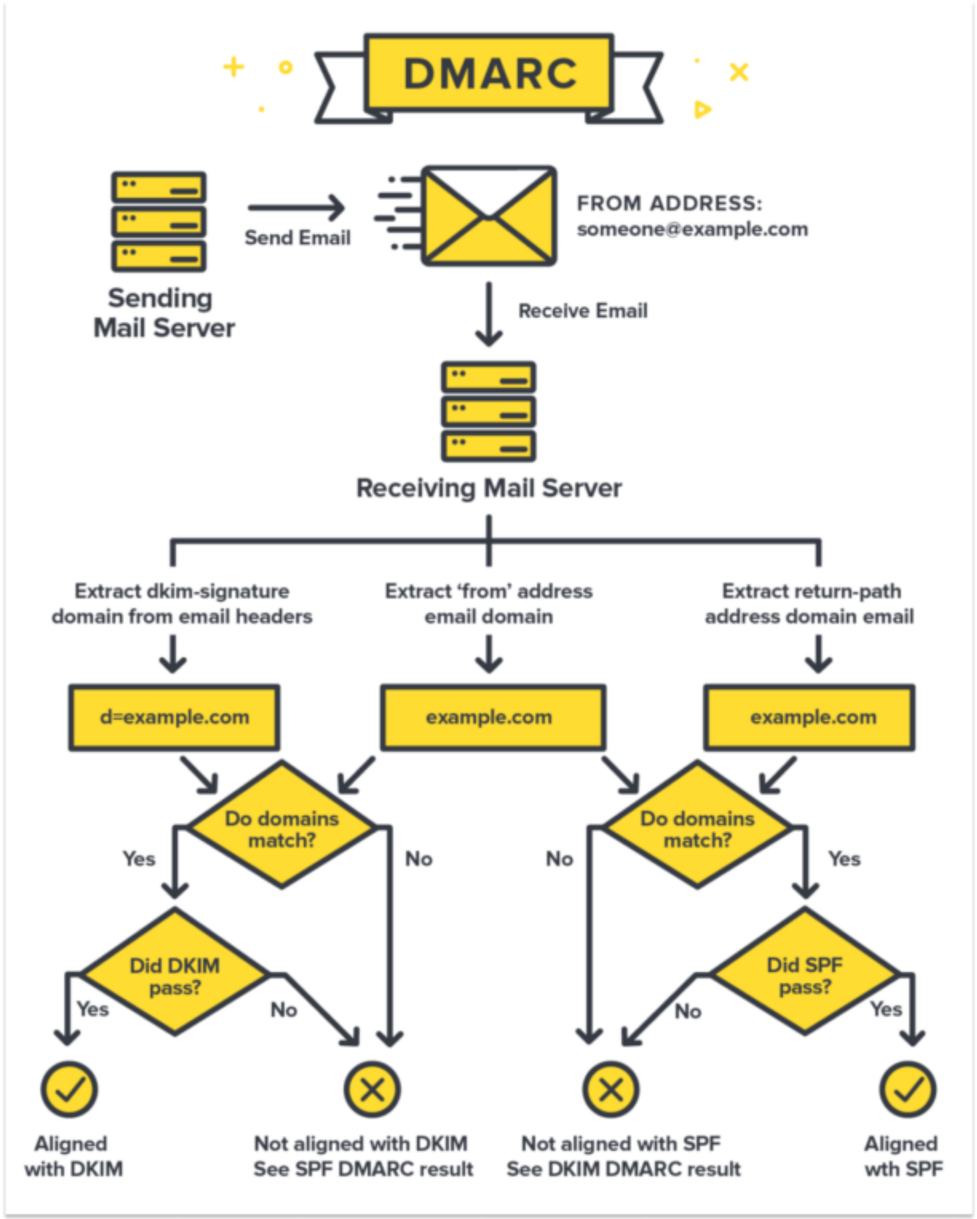


Diagram Credit: https://postmarkapp.com/guides/dmarc

DMARC Example

```
_dmarc.domain.com TXT v=DMARC1\; p=reject\; pct=100\; rua=mailto:dmarc-reports@domain.com\;
```

- _dmarc.domain.com: Denotes that this is a DMARC policy entry.
- v is the version
- p = Policy. In this case, reject. This means that any email that doesn't pass is rejected. None would only sends reports.
- rua is the reporting destination.

Examining Email Headers

Original Message

Message ID	<30955F7A-DFE4-4AC5-9ED1-F3934D80A4C0@datadistillr.com>
Created at:	Wed, Mar 22, 2023 at 10:51 AM (Delivered after 12 seconds)
From:	Charles Givre <charles@datadistillr.com> Using Apple Mail (2.3731.400.51.1.1)
To:	Charles Givre <cgivre@gmail.com>
Subject:	Testing
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain datadistillr.com Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

Examining Email Headers

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@datadistillr.com header.s=google header.b=ecdlFvjB;
       spf=pass (google.com: domain of charles@datadistillr.com designates
209.85.220.41 as permitted sender) smtp.mailfrom=charles@datadistillr.com;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=datadistillr.com
```

Examining Email Headers

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=datadistillr.com; s=google; t=1679496710;
        h=to:date:message-id:subject:mime-version:from:from:to:cc:subject
         :date:message-id:reply-to;
        bh=mDYcyhyMJxWHX8r9+ru6kyd6KtSQFHLEyrJu3ppaF98=;
        b=ecdlFvjBP2jG7gulCg51KkRrxIn0Grvm6XGTPJtq70hfEM5XOI9tJ6+hvjc2xY1oze
         F5+VNEZ7OOgfQsO0Zxg2eLNlnZv3Dj1JCSn4DIXtqA84F319x3TlbVdcZdSUKUyGazIq
         m075YZ+4GG5cowhMc3EugjgUKTnfIpjqqyY0o88h9b2USgsCoRW//ROxhVPTJZps+t7z
         JpAlN9pjWslpXQXLGb9EGePhi3x5uOAhVLU9JSFXt4enxhOkNsmEa3UxV7/4UY6F4Pw6
         /fhkTIj3NIY/sHxNvjxUAywcYvaSldC4CISEM0oZp1G8wVHem0Qci/+YpsRcPRb5E4Fl
         TmAA==
```

The Future...?

- Sometimes legitimate email servers will modify incoming messages, for instance, adding a warning if the sender is external to the organization. This can break DKIM.
- A new standard called Authenticated Received Chain (ARC). As of 2019 ARC is marked as experimental.
- You can think of ARC as DKIM but at every phase of the email process.

DNS Analytics in Python

Networking Analytics in Python

- Python offers you a robust set of modules to script DNS work.
- You can script most common DNS task to include reconnaissance, or domain management using python modules.

Networking Analytics in Python

- python-whois: As the name implies, python-whois enables you to gather whois information.
- tldextract: TLD extract is a utility module for parsing URLs and extracting portions from a URLs.
- dnspython: Module for executing DNS queries. You can use this module to gather information from DNS records, and maintain DNS records
- ipaddress: A built-in module for working with IP addresses.

Getting Whois Info in Python

- If you haven't installed it already, please install python whois:

```
pip install python-whois
```

- This module is very simple and produces a dictionary of values from the whois lookup.

Getting Whois Info in Python

```
import whois

w = whois.whois("gtkcyber.com")


{'domain_name': ['GTKCYBER.COM', 'gtkcyber.com'],
 'registrar': 'Google LLC',
 'whois_server': 'whois.google.com',
 'referral_url': None,
 'updated_date': datetime.datetime(2022, 3, 23, 19, 43, 19),
 'creation_date': datetime.datetime(2017, 1, 20, 3, 32, 35),
 'expiration_date': datetime.datetime(2024, 1, 20, 3, 32, 35),
 'name_servers': ['NS-CLOUD-B1.GOOGLEDOMAINS.COM',
  'NS-CLOUD-B2.GOOGLEDOMAINS.COM',
  'NS-CLOUD-B3.GOOGLEDOMAINS.COM',
  'NS-CLOUD-B4.GOOGLEDOMAINS.COM'],
 'status': ['ok https://icann.org/epp#ok', 'ok https://www.icann.org/epp#ok'],
 'emails': 'registrar-abuse@google.com',
 'dnssec': 'unsigned',
 'name': 'Contact Privacy Inc. Customer 7151571251',
 'org': 'Contact Privacy Inc. Customer 7151571251',
 'address': '96 Mowat Ave',
 'city': 'Toronto',
 'state': 'ON',
 'registrant_postal_code': 'M4K 3K1',
 'country': 'CA'}
```

Getting DNS Information

- Python has a very powerful module called dnspython which you can use to gather DNS information.
- If you haven't already, please install this with:

```
pip install dnspython
```

- With this module, we can find name servers, MX records, etc.

Executing a DNS Query

```
import dns
import dns.resolver

result = dns.resolver.resolve('hashnode.com', 'A')
A_records = []

for IPval in result:
    A_records.append(IPval.to_text())
print(A_records)
```

Executing a DNS Query

- When you execute DNS queries, different resolvers may produce different results. If the default resolver doesn't work for your domain, you may want to try different resolvers.
- There are a lot of things that can go wrong, so be sure to use try/catch blocks.
-

In Class Exercise: Worksheet 1

Questions?