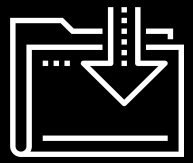
Email Networks and Security

Cybersecurity

Networking 2, Day 2



Class Objectives

By the end of today's class, you will be able to:

Domain Name Services (DNS), Validate DNS records using nslookup.

Describe the processes, protocols, and headers associated with email communication.

Analyze email headers to identify suspicious content.


Recap

Recap

Let's review how each of these networking concepts assists with transmitting data across networks to reach its destination.

- DHCP
- NAT
- Routing protocols
- Wireless

Today will build upon the previous class with networking concepts related to sending, receiving, and securing emails.

Today's Class

We will cover the following concepts:

First half of class

- The various DNS record types and how they assist with web browsing, sending and securing emails.
- Email protocols and the structure of an email.
- Email security issues and how to identify them.

Second half of class

All the networking concepts covered up to this point.

Addresses and the Internet

Accessing data from the internet applies similar network addressing concepts.

Domain Name System (DNS)

We will cover the following concepts:

Domain Name System

Domain Name System allows us to navigate to *facebook.com* instead of having to type *31.13.65.36*.

DNS Lookup

Using a process called **DNS lookup**, our browser searches a series of caches to find the IP address associated to the webpage we type.

Lookups and Caches

When a website is entered in a browser, the browser will check DNS caches to see if they already have the DNS translation of the domain's IP address stored.

Layers of Cache

The caches are searched in an ascending order of scope, starting at your browser's DNS cache and ending, if necessary, at the top-level domain DNS cache.

The DNS lookup process searches caches in the following order:

01 Browser's cache.

02 The operating system's cache, stored in the hosts file.

03 Internet Service Provider's (ISP) cache.

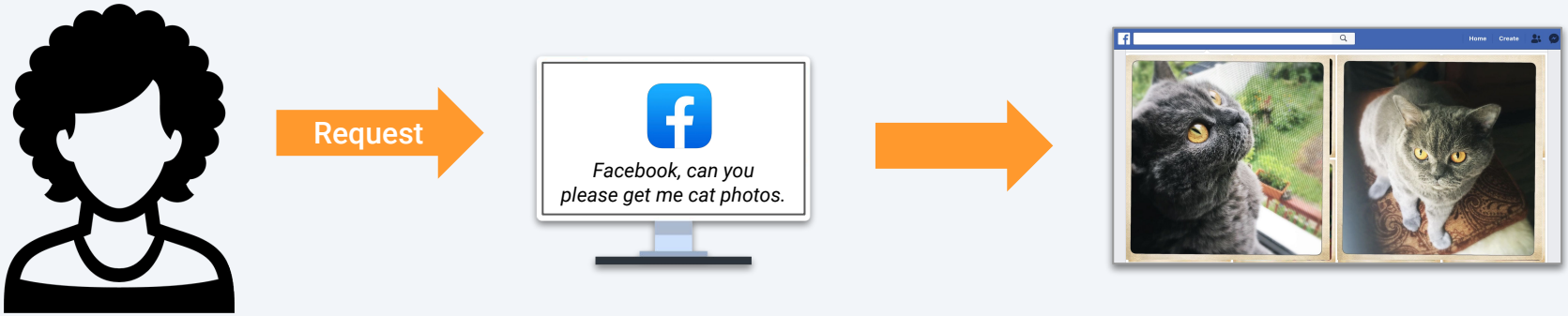
04 Finally, the top-level domain's (TLD) cache.

URLs

A domain is the website we access for resources. The resources we're requesting are typically at a specific location within that domain.

For example:

If we are viewing a picture from Facebook, the picture likely isn't located at the URL *www.facebook.com*. It is likely at a specific location, such as *www.facebook.com/photos/catpicture.jpg*.



URLs

This resource is located in the **URL (Uniform Resource Locator)**.

A URL is the full address of a resource on the internet.

Similar to file structures, URLs have a syntax indicating where to obtain the specific resource being requested.

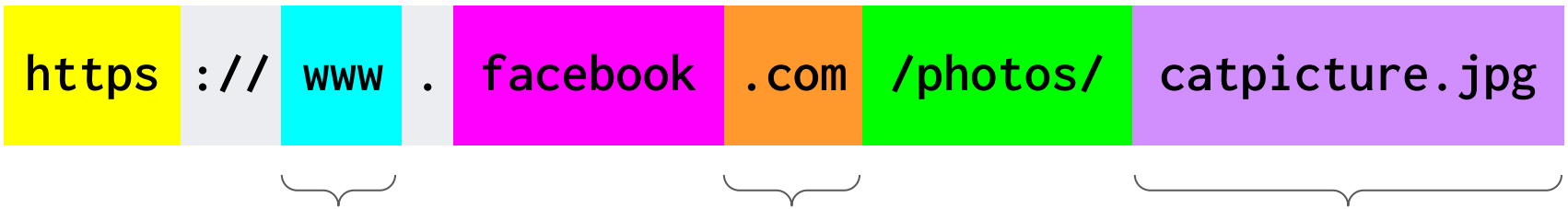
The syntax is: `[scheme]://[subdomain].[domain].[TLD][/path/][filename]`

URL Syntax

https
(Hypertext Transfer Protocol) is a scheme indicating a file on the internet.

facebook
is the primary domain.

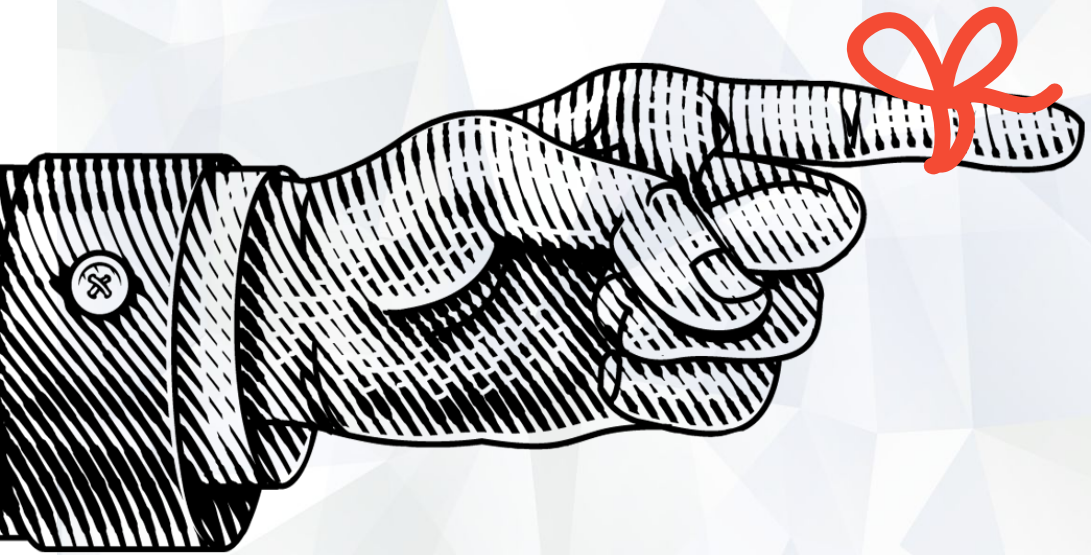
/photos/
is the path where the resource is located.



www
is a subdomain of facebook.com.

.com
is the TLD, or top-level domain.

catpicture.jpg
is the resource or file being requested.



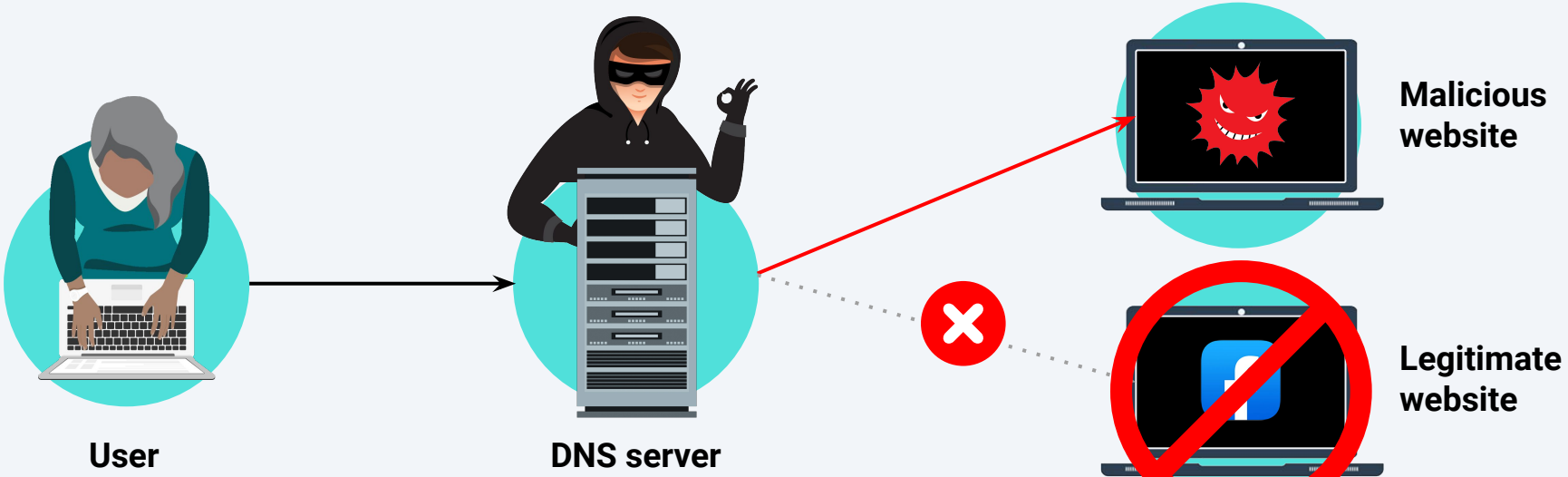
Remember,

- DNS caches indicate where to request the resources from, based on the domain being accessed.
- If a hacker is able to manipulate the DNS cache, they can trick and exploit a user's request by returning a domain or resource that was not originally requested.

DNS hijacking is a type of network attack that exploits DNS vulnerabilities to divert web traffic away from legitimate servers and towards fake or malicious servers.

DNS, URLs, and Security

Example: A hacker owns a malicious site located at the IP `137.74.187.102`.



The hacker accesses your hosts file DNS cache and updates a record that makes browser requests for facebook.com go instead to `137.74.187.102`.

Now, every time you go to facebook.com, you are redirected to the hacker's malicious website.

Instructor Demonstration

DNS Hijacking

Activity: DNS Hijackings

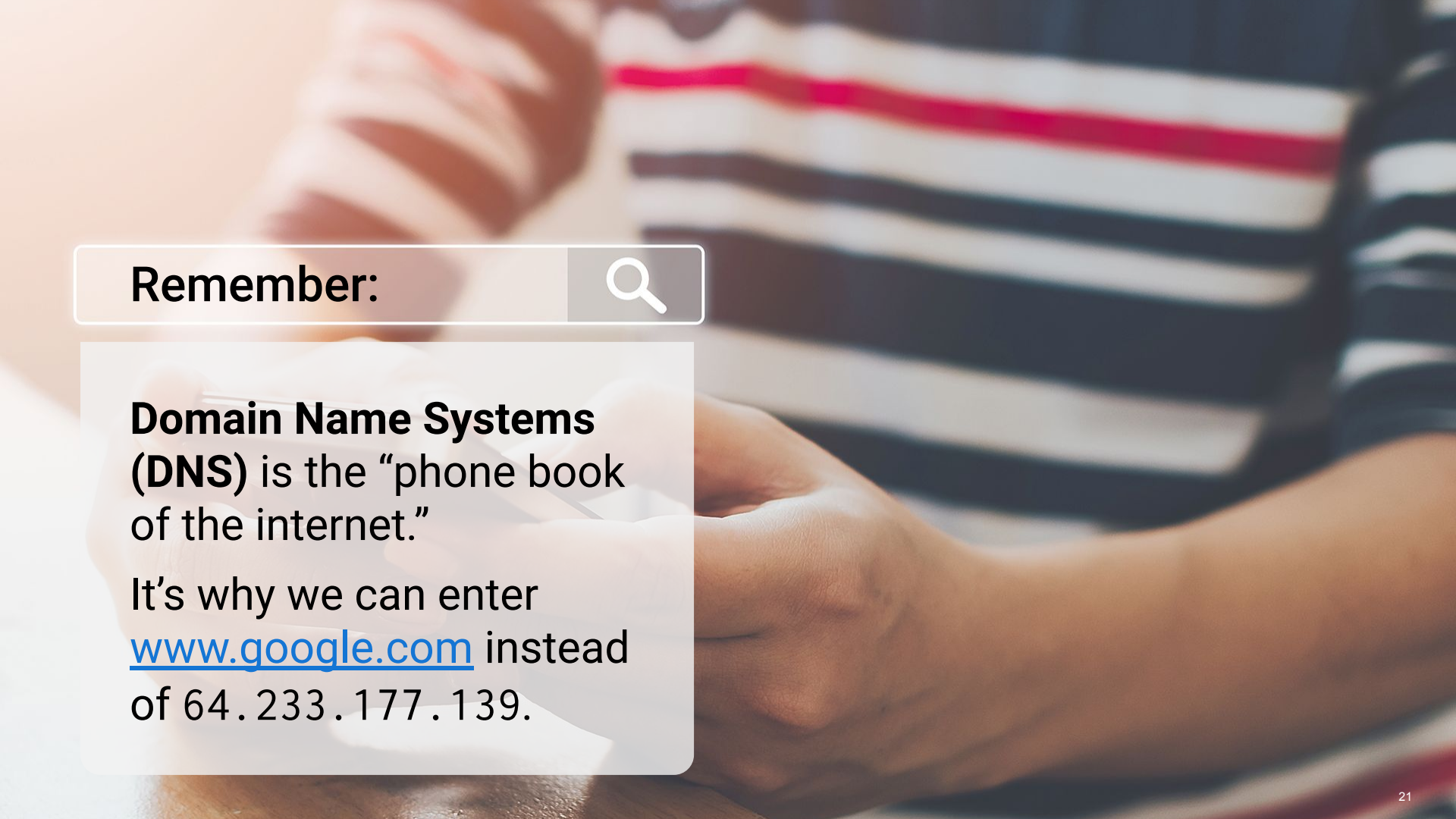
In this activity, you will continue to play the role of a security analyst at Acme Corp.

Your task is to create and test out a DNS spoof record that will redirect any hacker trying to visit acmetradesecrets.com to another website.

Suggested Time:

15 Minutes

DNS Record Types



Remember:

Domain Name Systems (DNS) is the “phone book of the internet.”

It’s why we can enter www.google.com instead of 64.233.177.139.

This translation of a domain to an IP address is a type of DNS record.

DNS Record Types

Occasionally, DNS needs to provide other details about a domain.

For example:

When you send an email, your email server needs to find the mail server name for the domain receiving the email. These details are provided by the many other DNS record types.

A **DNS zone file** is an actual file containing all the DNS records for a particular domain.

DNS Zone File

A DNS zone file lives in a DNS server.

A DNS zone file contains a **Time to Live (TTL)** indicating how long a **DNS cache** will remember the information in the file before having to request an updated copy from the DNS server.

A DNS zone file also contains the DNS records with information about the domain.

DNS Record Types

While there are many available DNS records types, a handful of common DNS records types are important to know:

DNS Record Type	Definition	Example
A record	Translates a domain to an IP address.	An A record for widgets.com points to `23.43.54.234`.
PTR record	The opposite of an A record, the PTR record translates an IP address into a domain.	The PTR record of `23.43.54.234` points to widgets.com.
CNAME record (*canonical name*)	An alias record used to point one domain to another domain.	A CNAME record pointing widgets2.com to widgets.com so a second DNS record doesn't need to be created for widgets2.com.

DNS Record Types

DNS Record Type	Definition	Example
SOA record (*start of authority*)	Contains administrative details about a domain.	• Email address of the administrator • TTL value • When the domain was last updated
NS record (*name server*)	Indicates which server contains actual DNS records for a domain. Also known as authoritative **name server**.	A device wants to know the IP address for widgets.com, and makes a DNS request asking which authoritative name server is for widgets.com. Once the **NS record** is confirmed, the device can trust this record for obtaining the IP address (or any other DNS record type) from the domain widgets.com.

NS Records

Domain

A domain can have multiple NS records for redundancy (if one fails, another is available).

For example:

widgets.com has two name servers containing its DNS records:

- `ns1.dnscompany.com`
- `ns2.dnscompany.com`

Subdomain

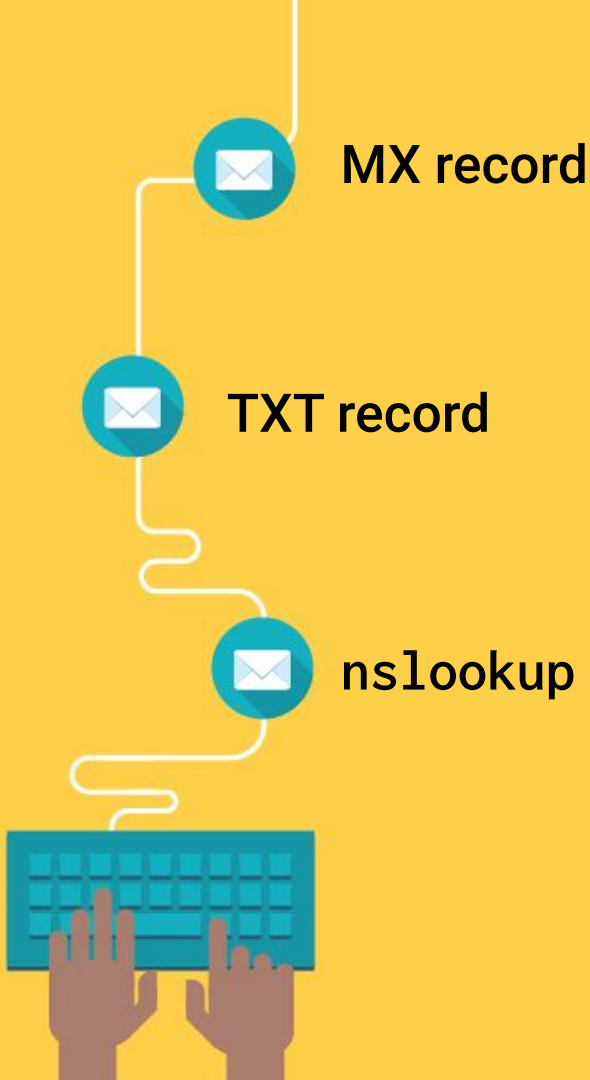
NS records can also be used to point subdomains to name servers.

For example:

We can point the subdomain **marketing.widgets.com** to a DNS server of `ns3.dnscompany.com`.

DNS Records and Email Communication

Some DNS record types assist with email communications.



MX record (*mail exchange*) directs emails to a specific mail server for a domain.

MX Record: Example

widgets.com has a mail server called **mailhost.widgets.com**.

If an email is sent to **bob@widgets.com**, the sender will validate that the MX record for **widgets.com** is **mailhost.widgets.com**.

The sender then directs the email to the mail server mailhost.widgets.com.

Just like NS records, domains can have multiple MX records for redundancy, in case one goes down or can't handle a large amount of traffic.

MX Records: Preferences

MX records have **preferences** for setting the primary and secondary mail servers.

These preferences are set with numerical **preference numbers** in front of the mail server name. The lower the preference number, the higher the priority.

For example: gadgets.com has the following MX records:

`10 mailhost_Atlanta.gadgets.com`	02	If the New York server is down, it will try Atlanta.
`5 mailhost_NewYork.gadgets.com`	01	An incoming email is received by the New York server, which has the **lowest preference number**.
`20 mailhost_LA.gadgets.com`	03	If Atlanta is down, it will try the LA mail server.

TXT record (*text*) was created to include human-readable notes, such as associated company name. These also include computer-readable data.

TXT Record Example

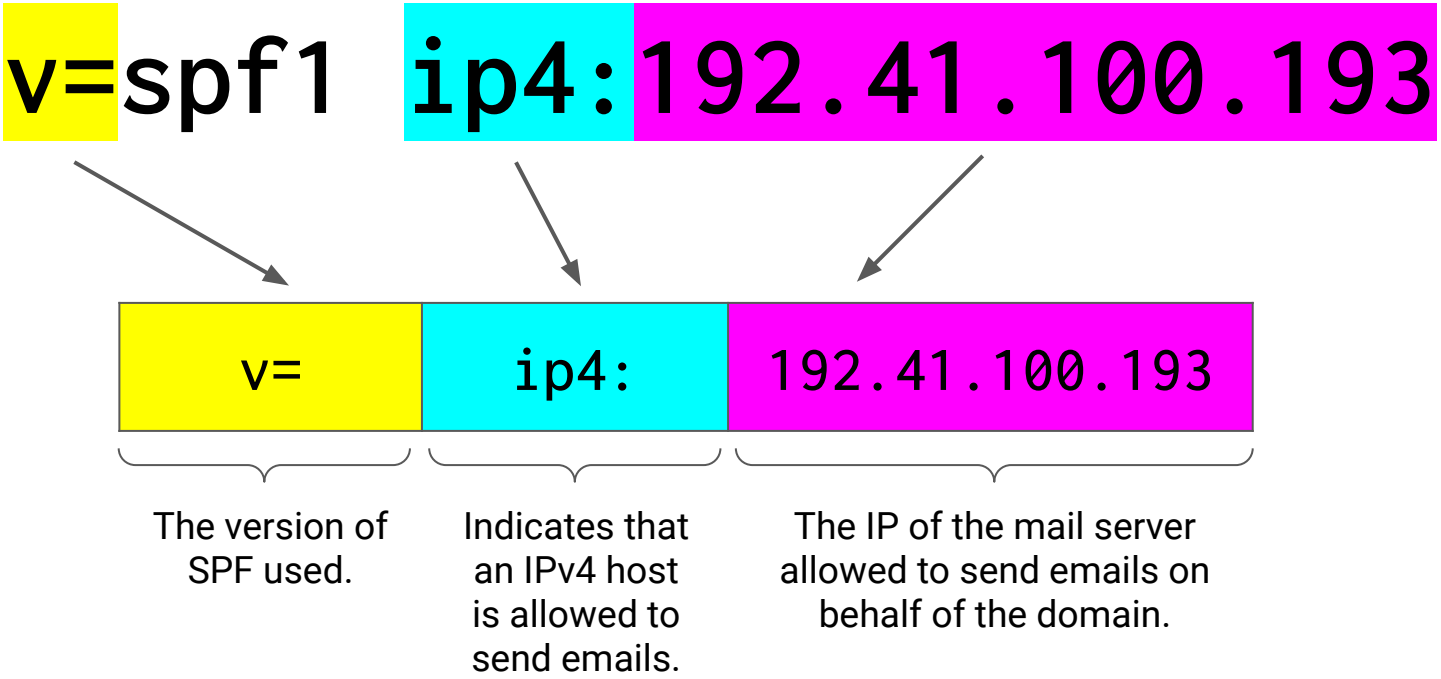
An example of computer-readable TXT data is the **SPF record** (*sender policy framework*), which determines if an email is from a trusted server.

An SPF record indicates which mail servers are allowed to send emails on behalf of a domain.

An SPF record's main purpose is to prevent spam, phishing, and email spoofing, by detecting emails that may have a forged sender email.

Not all organizations send emails from mail servers within their domain. Their mail servers may exist in another domain, or another organization may send marketing emails on behalf of an organization.

SPF Record Example



How SPF Records Work

widgets.com's DNS SPF record indicates that `23.43.54.235` and `23.43.54.236` are the IP addresses of mail servers allowed to send emails on its behalf.

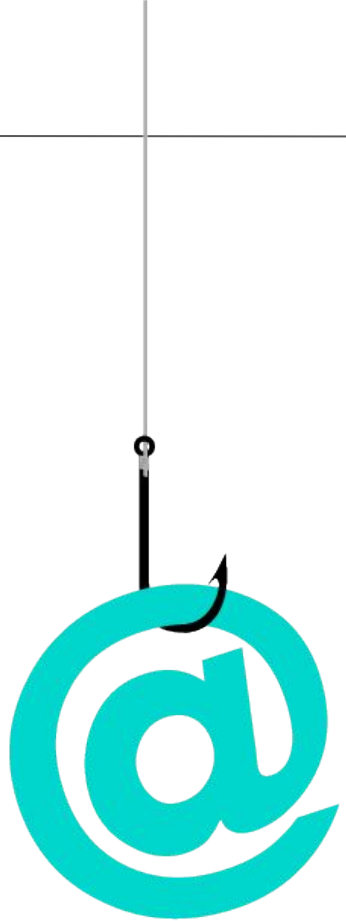
gadgets.com received a suspicious email from a **widgets.com email**.

When the receiving email server at **gadgets.com** receives the email, it completes the following steps:

01 Checks the sending mail server's IP address, `12.54.54.23`.

02 Validates the DNS record of **widget.com's** SPF record to confirm the sending mail server's IP address is either `23.43.54.235` or `23.43.54.236`.

03 Since the sender's IP is `12.54.54.23` (not `23.43.54.235` or `23.43.54.236`), gadgets.com's mail server can identify the email as spam and potentially reject it or send it to the recipient's spam folder.



nslookup (*name server lookup*) allows us to easily look up the DNS records of any domain.

nslookup

If emails aren't reaching their final destination, we could check the MX records for a particular DNS domain to make sure the settings are accurate.

The command-line tool **`nslookup`** (*name server lookup*) allows us to easily look up the DNS records of any domain.

The **`nslookup`** tool is available on most operating systems without having to be installed.

To specify just MX records, use `set type=mx` within nslookup.

```
ryan@Computer:~$ nslookup
> set type=mx
> google.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
```

Instructor Demonstration

nslookup Walkthrough

Activity: DNS Record Types

In this activity, you will continue to play the role of a security analyst at Acme Corp.

Acme Corp recently updated several domain DNS records.

Your task is to use **`nslookup`** to validate the updates of the DNS records for each of the domains provided.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Questions?

Introduction to Email Networking

Introduction to Email Networking

While it seems simple to send an email from one address to another, there are many processes and technologies working in the background to make this magic happen. Understanding how this detailed process works can assist network and security professionals in identifying email issues or attacks.

How Email Works

Step 1

Bob uses Microsoft Outlook to type and send an email to Alice.

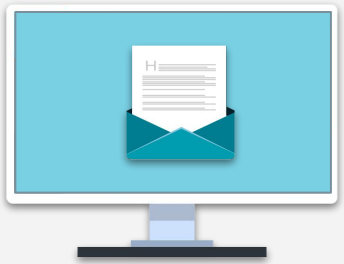
Step 2

Bob's mail server finds Alice's mail server.

Step 3

Bob's mail server forwards the email to Alice's mail server.

Step 4



Alice pulls Bob's email onto her local computer to read it.

How Email Works

Step 1

Bob uses Microsoft Outlook to type and send an email to Alice.

- Bob, whose email is **Bob@bob.com**, composes an email to send to Alice, whose email is **Alice@alice.com**.
- Once Bob clicks **Send**, the email is forwarded to Bob's company's email server.
- The email server is also referred to as the **MTA** (mail transfer agent).

How Email Works

Step 2

Bob’s mail server finds Alice’s mail server.

- Bob’s mail server does a DNS lookup against **alice.com** to determine its mail server.
- Bob’s mail server gets this information from **alice.com’s** MX record.

How Email Works

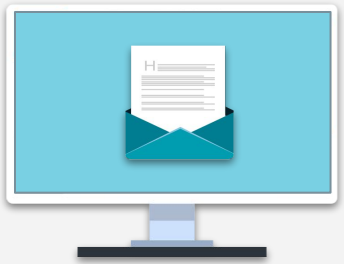
Step 3

Bob’s mail server forwards the email to Alice's mail server.

- Using a protocol called SMTP (Simple Mail Transfer Protocol), Bob’s mail server sends the email to Alice’s mail server.
- SMTP uses port 25 and is part of **Layer 7: Application** of the OSI model.

How Email Works

Step 4



Alice pulls Bob's email onto her local computer to read it.

- Bob's email is currently sitting on Alice's email server, and Alice needs to pull it from this server in order to read it.
- Two protocols can be used to transfer the email to Alice's local computer: **POP3** and **IMAP**.

POP3 vs. IMAP

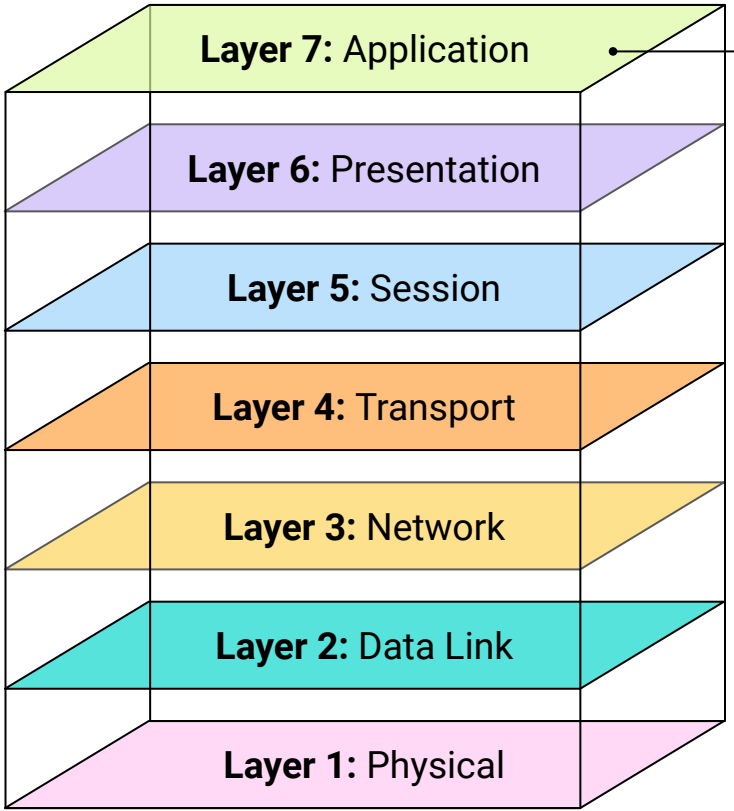
POP3

- With POP3 (Post Office Protocol), when Alice logs in and checks her email from Bob, the POP3 mailbox doesn't keep a copy of the email.
- Alice would not be able to log in to another computer and view Bob’s email, as it already has been downloaded from the mail server.
- POP3 has a security benefit, as the email will not exist on a server the recipient doesn’t control.

IMAP

- With IMAP (Internet Message Access Protocol), a copy of the email is kept on the server.
- Even after Alice logs in and checks her email from Bob, she can check it again from another computer.
- IMAP has the benefit of preventing data from being lost, as it backs up emails on a server.

POP3 and IMAP



Both POP3 and IMAP are part of **Layer 7: Application** of the OSI model:

- POP3 uses port `110`
- IMAP uses port `143`

Understanding these steps is important for diagnosing and troubleshooting email issues.

Email Headers

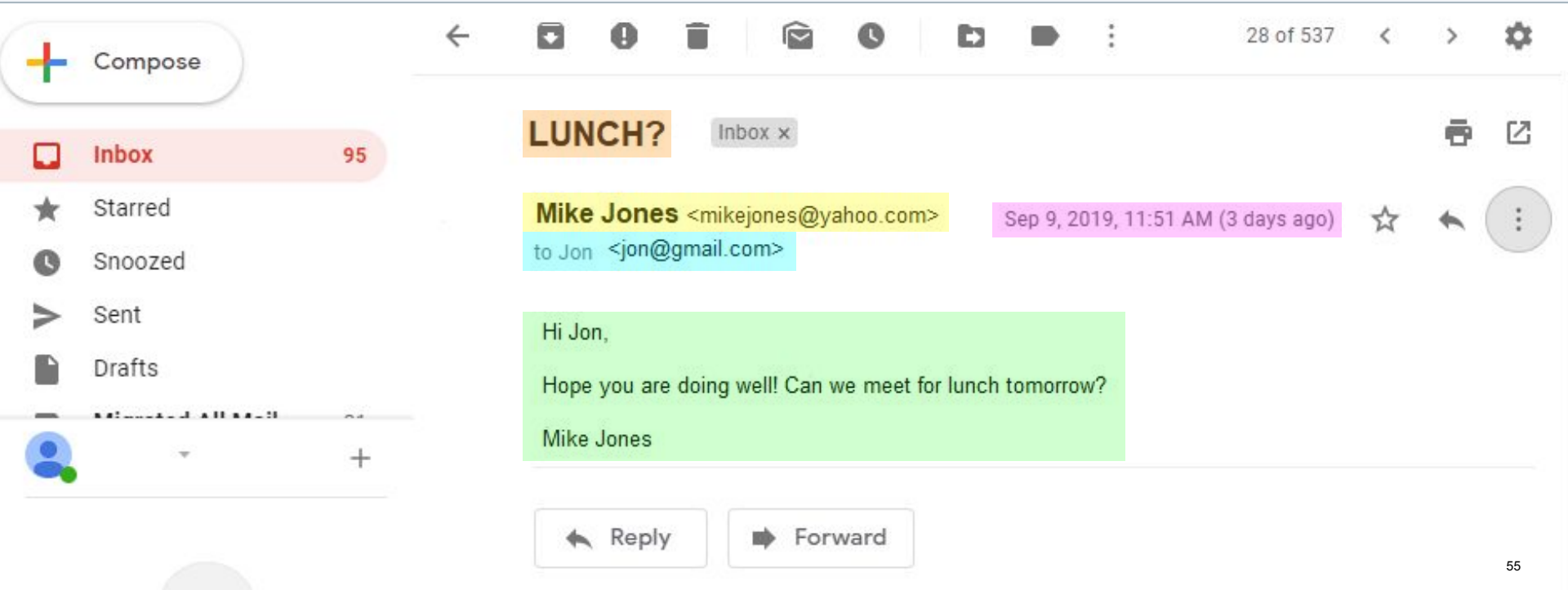
There are many **header** fields that can be used for emails, some required and some optional.

From email address	(Required) The email of the sender.
To email address	(Required) The required email of the recipient.
Email subject	(Optional) The field for describing the subject of the email.
Email message body	(Optional) The field containing the message.
Date/Time	Date and time the email was sent. This is added by the email client.

Familiar Fields

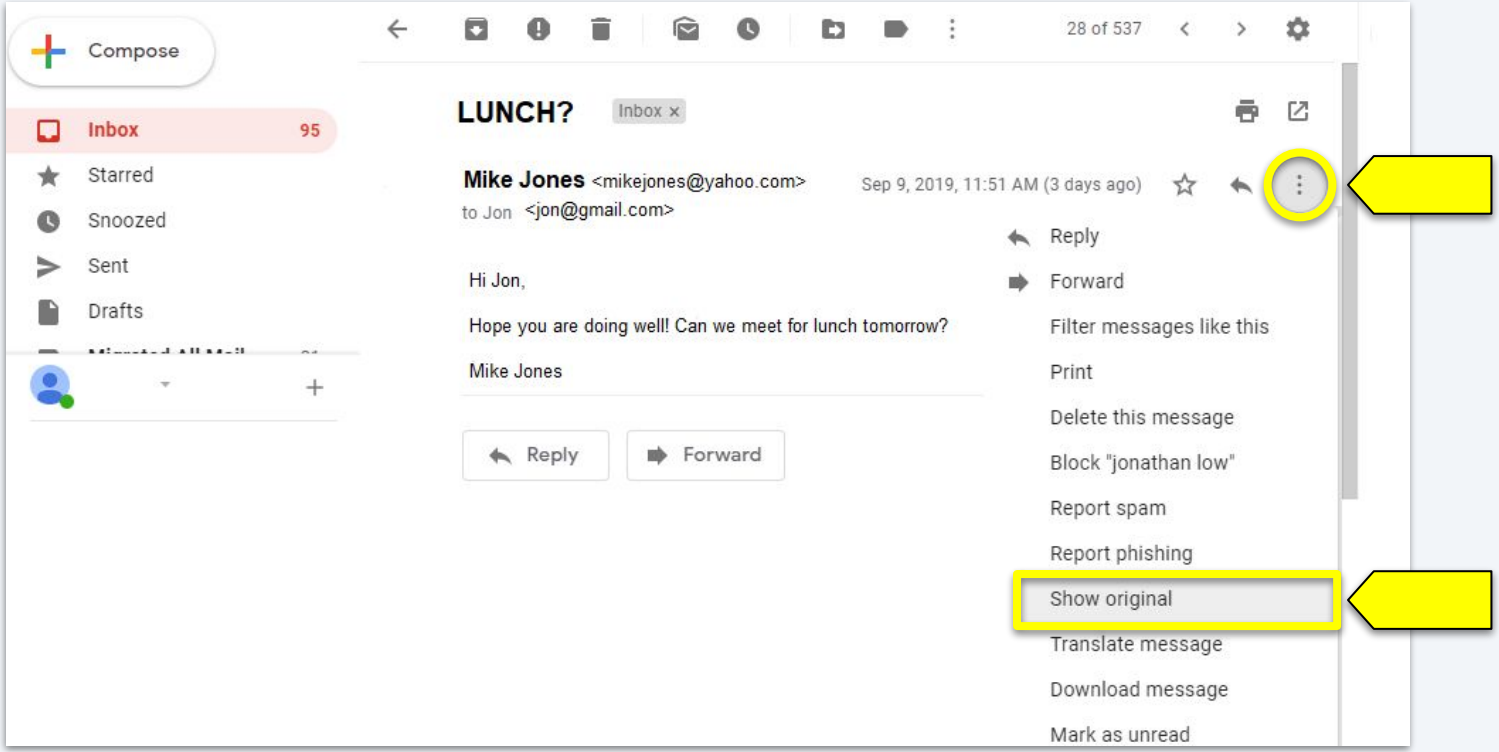
If you've ever sent an email, you're probably familiar with the following fields:

From email address | To email address | Email subject | Email message body | Date/Time



Unfamiliar Fields

More fields are revealed by reviewing the complete raw email:

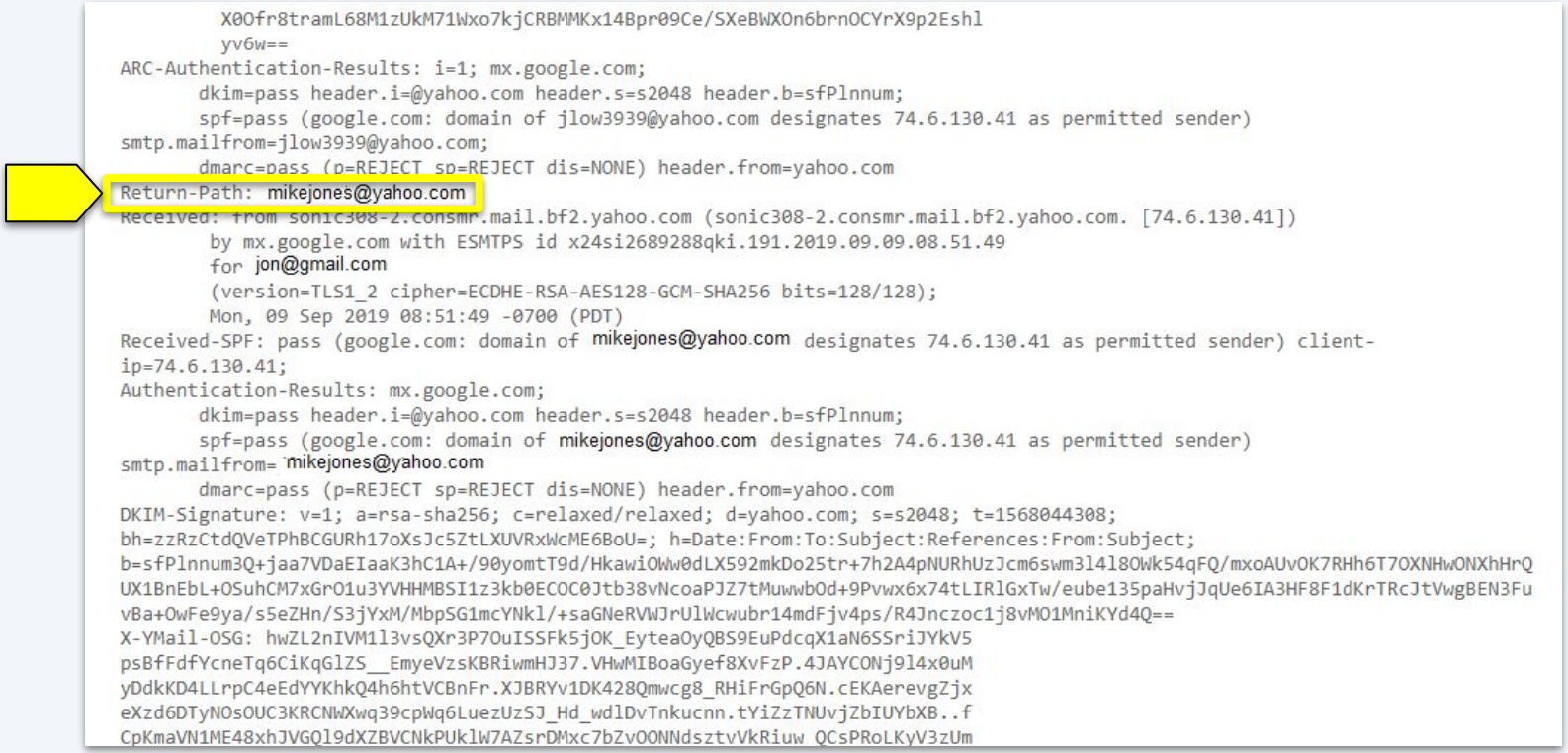


Unfamiliar Fields

Delivered-To: Specifies the recipient's email.

Unfamiliar Fields

Return-Path: Specifies the sender's return email.



```
        X0Ofr8tramL68M1zUkM71Wxo7kjCRBMMKx14Bpr09Ce/SXeBWXOn6brnOCYrX9p2Eshl
        yv6w==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of jlow3939@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom=jlow3939@yahoo.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
Return-Path: mikejones@yahoo.com
Received: from sonic308-2.consmr.mail.bf2.yahoo.com (sonic308-2.consmr.mail.bf2.yahoo.com. [74.6.130.41])
        by mx.google.com with ESMTPS id x24si2689288qki.191.2019.09.09.08.51.49
        for jon@gmail.com
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 09 Sep 2019 08:51:49 -0700 (PDT)
Received-SPF: pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender) client-
ip=74.6.130.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com header.s=s2048 header.b=sfPlnnum;
       spf=pass (google.com: domain of mikejones@yahoo.com designates 74.6.130.41 as permitted sender)
smtp.mailfrom=mikejones@yahoo.com
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1568044308;
bh=zzRzCtdQVeTPhBCGURh17oXsJc5ZtLXUVRxWcME6BoU=; h=Date:From:To:Subject:References:From:Subject;
b=sfPlnnum3Q+jaa7VDaEIaaK3hC1A+/90yomtT9d/HkawiOWw0dLX592mkDo25tr+7h2A4pNURhUzJcm6swm3l4l8OWk54qFQ/mxoAUvOK7RHh6T7OXNHwONXhHrQ
UX1BnEbL+OSuhCM7xGrO1u3YVHHMBSI1z3kb0ECOC0Jtb38vNcoaPJZ7tMuwwbOd+9Pvwx6x74tLIRlGxTw/eube135paHvjJqUe6IA3HF8F1dKrTRcJtVwgBEN3Fu
vBa+OwFe9ya/s5eZHn/S3jYxM/MbpSG1mcYNkl/+saGNeRVWJrUlWcwubr14mdFjv4ps/R4Jnczoc1j8vMO1MniKYd4Q==
X-YMail-OSG: hwZL2nIVM1l3vsQXr3P7OuISSFk5jOK_EyteaOyQBS9EuPdcqX1aN6SSriJYkV5
psBfFdfYcneTq6CiKqGlZS__EmyeVzsKBRiwmHJ37.VHwMIBoaGyef8XvFzP.4JAYCONj9l4x0uM
yDdkKD4LLrpC4eEdYYKhkQ4h6htVCBnFr.XJBRYv1DK428Qmwcg8_RHiFrGpQ6N.cEKAerevgZjx
eXzd6DTyNOsOUC3KRCNWXwq39cpWq6LuezUzSJ_Hd_wdlDvTnkucnn.tYiZzTNUvjZbIUYbXB..f
CpKmaVN1ME48xhJVGQl9dXZBVCNkPUklW7AZsrDMxc7bZvOONNdsztvVkRiuw_QCsPRoLKyV3zUm
```

Unfamiliar Fields

Received: Shows a list of mail servers, illustrating the path taken by the email from its source to destination.

Unfamiliar Fields

Message-ID: Unique string created by the sending mail server as an identifier of the email

Received SPF: The SPF verification field

Unfamiliar Fields

You may notice email headers that begin with an “x”, such as: **x-mailer**, **x-Google-Smtp-Source**.

The “x” signifies an extension of the standard headers.

These header records are optional and are typically used for custom applications.

They can also provide additional services for tracking, reporting, and authentication.

Activity: Email Networking

In this activity, you will continue to play the role of a security analyst at Acme Corp.

Your task is to analyze the header records of suspicious emails and document several data points.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Email Security Issues

Email Security Issues

While email provides many benefits, it also comes with many security concerns.

One of the top email concerns for most users and businesses is spam: “the sending of unsolicited emails.”

Email Security Issues: Spam

Over 60% of all emails can be identified as spam.

- While spam isn't inherently dangerous, a large number of spam emails can be very inconvenient for organizations.
- Many email systems have developed advanced methods for detecting and stopping spam emails.
- These methods involve using SPF records, matching lists of known spam senders, and keyword identification.

Email Security Issues: Unencrypted Channels

Emails are almost always not encrypted.

Emails are typically routed across multiple mail servers before reaching their destinations, opening up the risk of email interception and viewing by unauthorized parties.

Several technologies can be used to encrypt confidential emails such as:

PGP	Pretty Good Privacy
S/MIME	Secure/Multipurpose Internet Mail Extensions

The challenge of PGP and S/MIME is that they involve coordination and setup between the email sender and the email receiver.

Email spoofing is when an email is designed to trick the receiver into believing it is coming from a trusted source.

Email Security Issues: Email Spoofing

Phishing—the attempt to gain sensitive information from an email recipient—is often accomplished through email spoofing.

A scammer sends you an email pretending to be from your bank.

The email asks you to update your username and password.

At first glance, the spoofed email looks like it legitimately came from your bank.

The email may contain a phishing URL that has a fake bank login page, which maliciously captures your banking username and password.

According to a recent report from Microsoft:

Phishing attacks are by far the most common cybersecurity threat— increasing a massive 250% since the previous report was published.

CPO Magazine

Source: CPO Magazine

Email Security Issues: Email Spoofing

Fortunately email spoofing can be detected with several methods, which analyze the raw email headers in sent emails.

01 the *From* Email Header

02 the *Received-SPF* Email Header

03 the *Received* Email Header

Method 1: the *From* Email Header

Spammers and phishers often disguise their true source email, changing the displayed email source to a name the recipient will trust or recognize.

For example:

You check your inbox and see an email from “Citibank.”

When you view the raw email header in either the “From” field, or the “Return-Path,” the true email address of the sender is displayed.

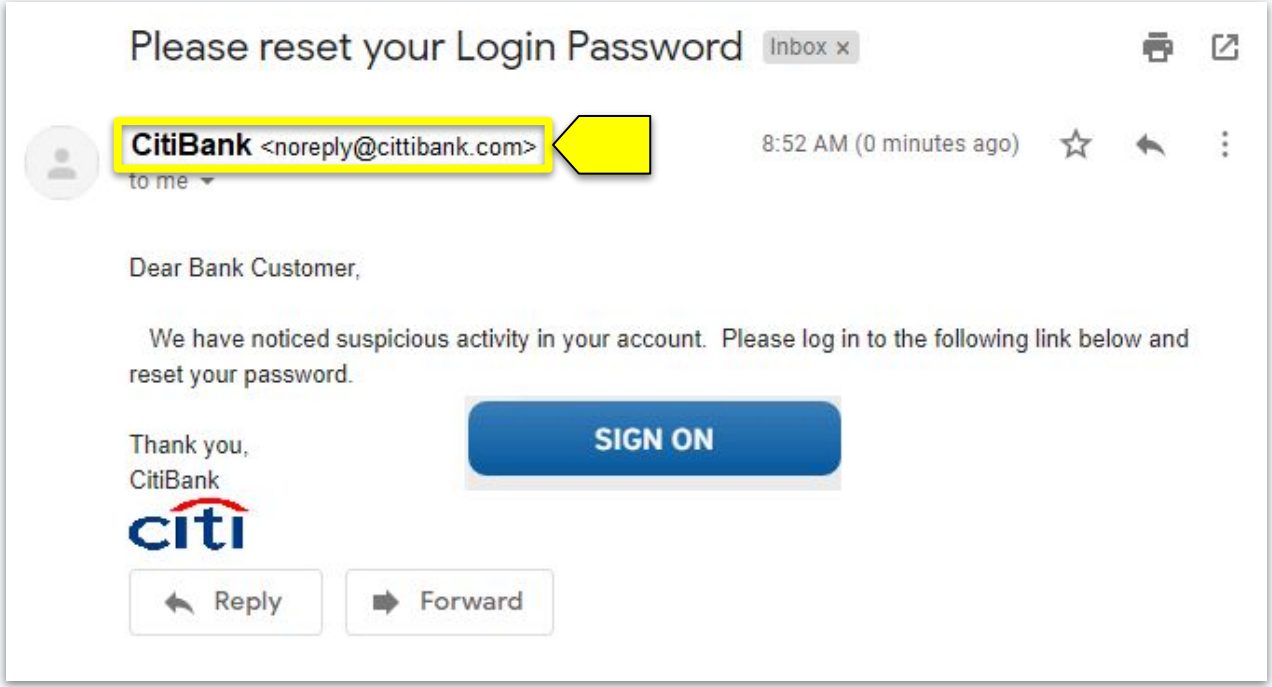
The email address is `sdfs2344dsf@yahoo.com`—it doesn’t have a `@citibank` domain. This is an indicator of a malicious email.

Method 1: the *From* Email Header

Another method used by phishers is to make a slight change to the name of the sending domain.

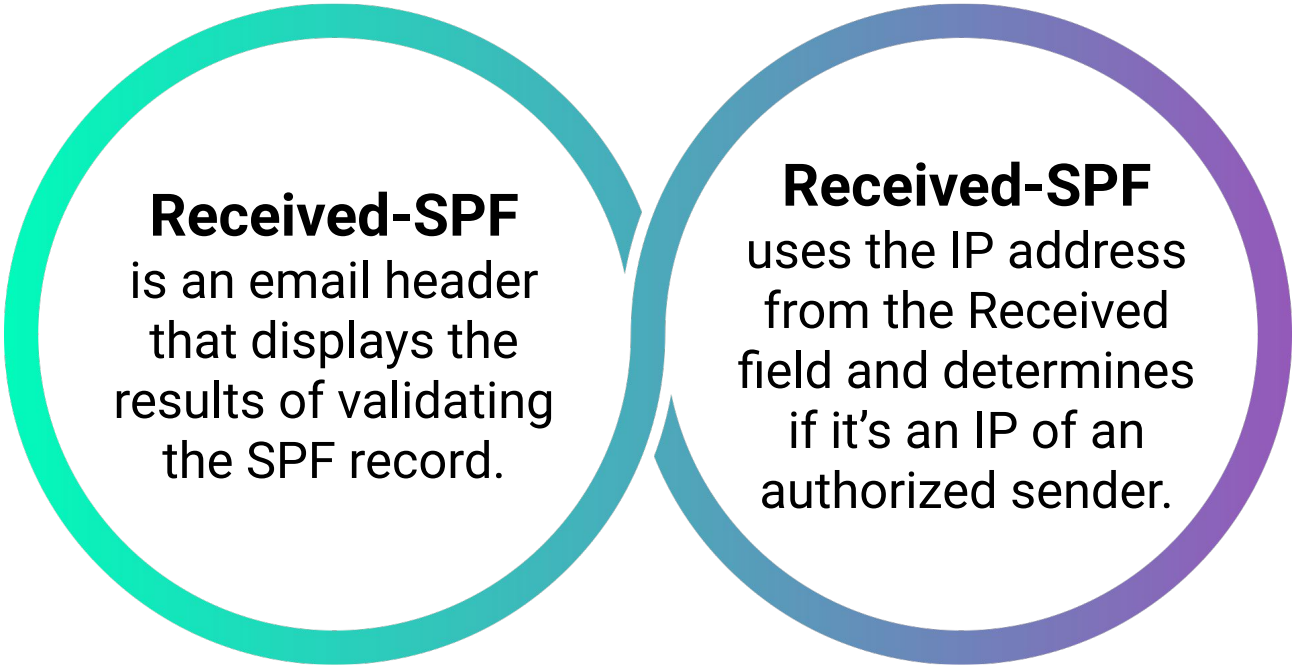
Look closely at the email for any small misspellings.

For example, a phisher could use the from email domain of @cittibank.com, with an additional “t” in the domain.



Method 2: the *Received-SPF* Email Header

As we mentioned earlier, the SPF record is used identify which mail servers are authorized to send emails on behalf of a domain.



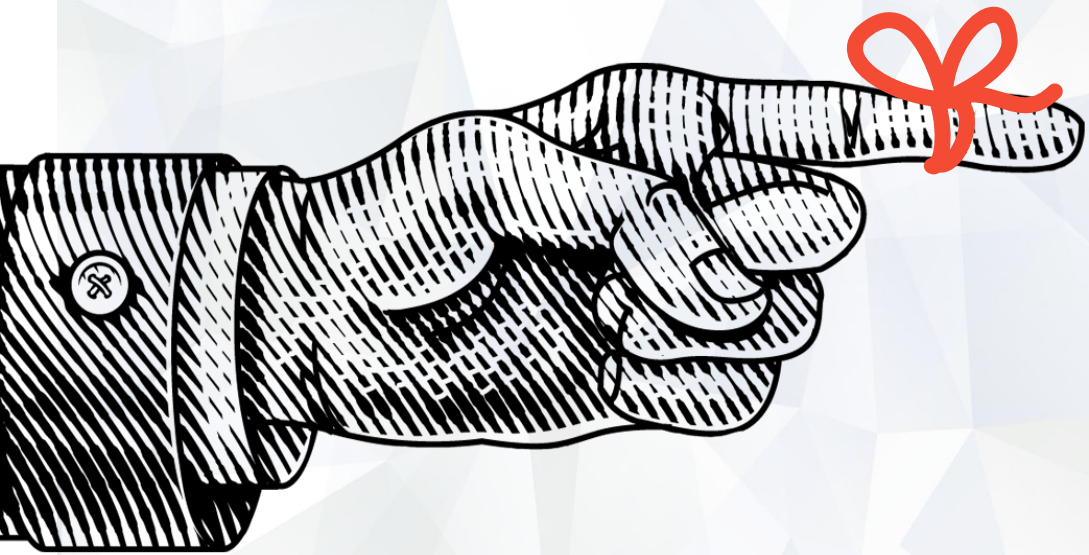
Method 2: the *Received-SPF* Email Header

If the IP is accepted it will display as a **“pass.”**

```
Received-SPF: pass (google.com: domain of michael@acme.com
designates 76.87.4.15 as permitted sender)
```

If the IP is not accepted it will display as a **“fail.”**

```
Received-SPF: fail (google.com: domain of michael@acmers.com
does not designate 174.81.74.11 as permitted sender)
```



Remember,

The *Received* header includes the source IP of the mail server that sent the email.

Method 3: the *Received* Email Header

There are many web tools available to look up IP address information.

For example, the ARIN Whois/RDAP tool.

While this isn't always the simplest way to validate a legitimate email sender, it is used by security professionals to provide additional information about the sender.

Method 3: the *Received* Email Header

ARIN Whois/RDAP tool example:

- You receive an email from a US-based government organization, such as the IRS.
- The IP address from the Received header record is `41.32.23.52`.
- Looking up this IP on arin.net shows the location of the IP is Egypt.
- This indicates that the email is probably not legitimate, as it's unlikely that a US-based government organization would have a mail server based in Africa.

Method 3: the *Received* Email Header

Many email systems have built-in technologies that automate methods to identify and detect spoofed and phishing emails.

- These automated systems aren't perfect, and can miss spoofed and phishing emails.
- It's important for security professionals to understand how to use these methods themselves.

Activity: Email Security

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You must further analyze the emails to determine which are spoofed and which are legitimate.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Questions?

Countdown timer

15:00

(with alarm)

⚠️ Heads Up ⚠️

The remaining activities are reviews of the concepts from the previous two units. These are optional and can be completed if time remains.

For the remainder of class, we will review the networking concepts covered in the previous networking classes.

Activity: Networking Concepts Review

In this activity, you will review the most important topics of the past few classes: HTTP, ARP, DHCP, TCP, and UDP; network devices, topologies, and routing; and network addressing.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?

Activity: Networking Attacks Review

In this activity, you will review ARP, DHCP, TCP, wireless, and email attacks.

Suggested Time:

15 Minutes

Time's Up! Let's Review.

Questions?


The End