Assignment 1 - Hands-On

Sam Peller

August 12, 2024

ISM 4323

Project 1-1: Examining data breaches visual

Objective: Explain the security concerns associated with various types of vulnerabilities

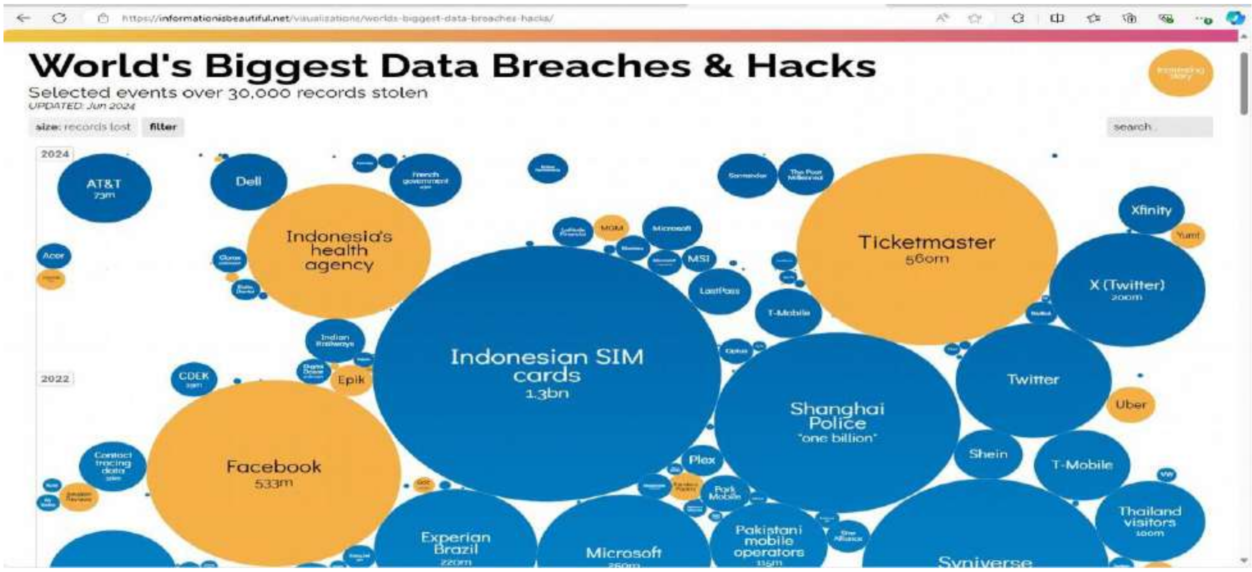
Description: In this project, you use a visual format to view the biggest data breaches resulting in stolen information.

Introduction

When it comes to Network Security there are many avenues' people will take to try and gain access to sensitive information. This also comes with many associated security concerns and vulnerabilities that consistently need to be monitored to keep private information private. As a result of some massive data breaches, companies can lose their futures, and people can lose their privacy as well as their money. This will go over some of the biggest data breaches and the resulting information stolen.

1. Open your web browser and enter the URL www.informationisbeautiful.net/visualizations/worlds-biggestdata-breaches-hacks/ (If you are no longer able to access the site through this web address, use a search engine to search for "Information Is Beautiful World's Biggest Data Breaches & Hacks.")

2. This site will display a visual graphic of the data breaches, as shown in Figure 1-7.



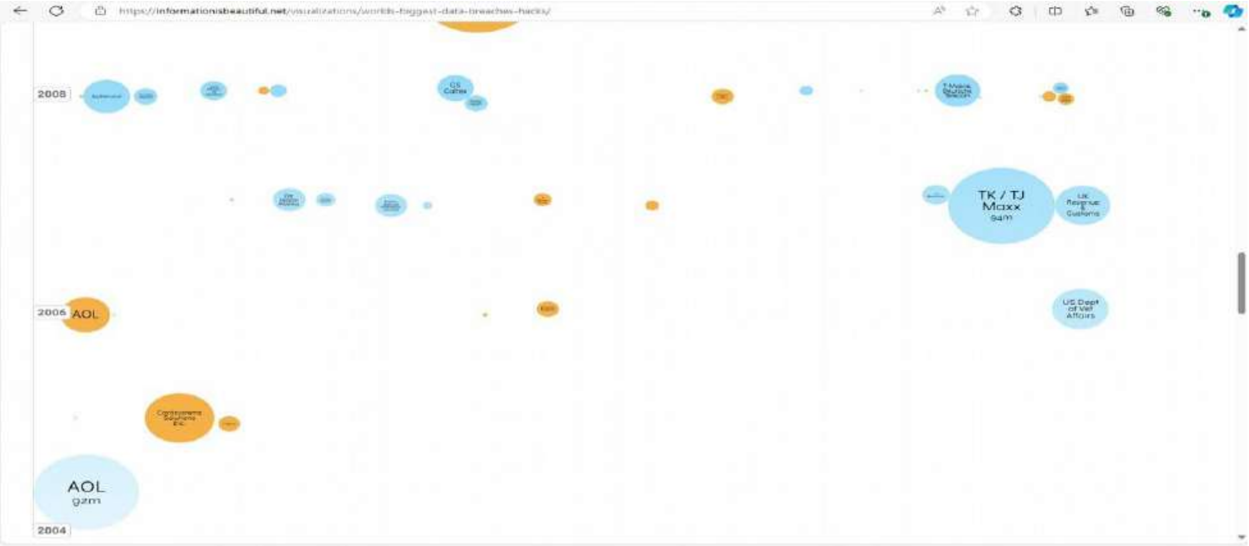
https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records stolen

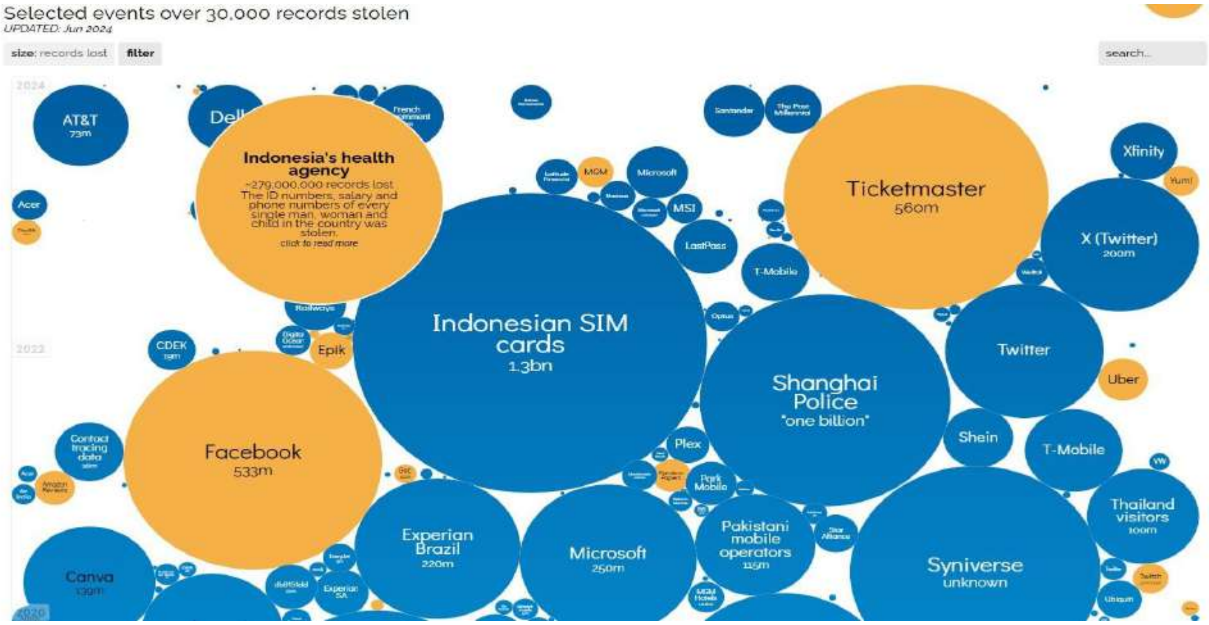
UPDATED: Jun 2024

3. Scroll down the page to view the data breaches by year. Note that the size of the breach is indicated by the size of the bubble.


https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
2008
T-Mobile Deutsche Telecom
TK / TJ Maxx
94m
UK Revenue Customs
2006
AOL
US Dept of Vet Affairs
Cardsystems Solutions Inc.
AOL
92m
2004

4. Scroll back up to the top.

5. Hover over several of the bubbles to read a quick story of the breach.


Selected events over 30,000 records stolen

UPDATED: Jun 2024

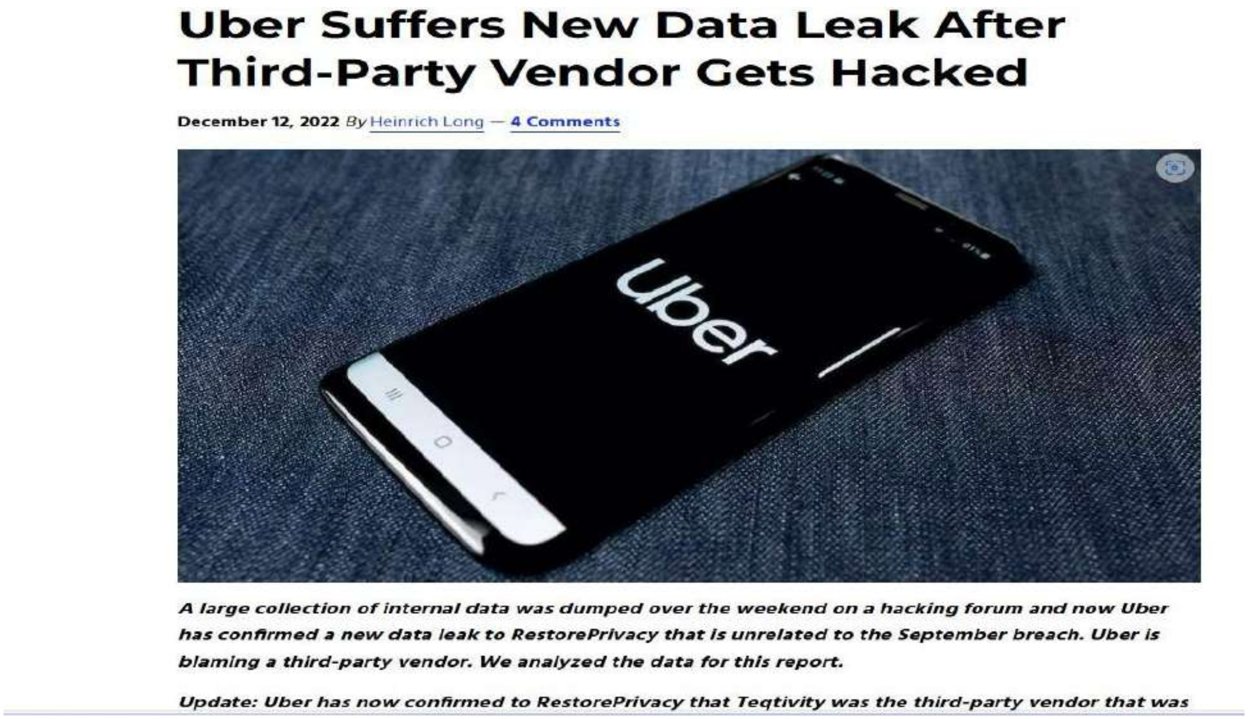
Indonesia's health agency

~279,000,000 records lost

The ID numbers, salary and phone numbers of every single man, woman and child in the country was stolen.

click to read more

6. Note the color of the bubbles that have an "Interesting Story." Click one of the bubbles and read the story. When finished, close only the interesting story tab in your browser.



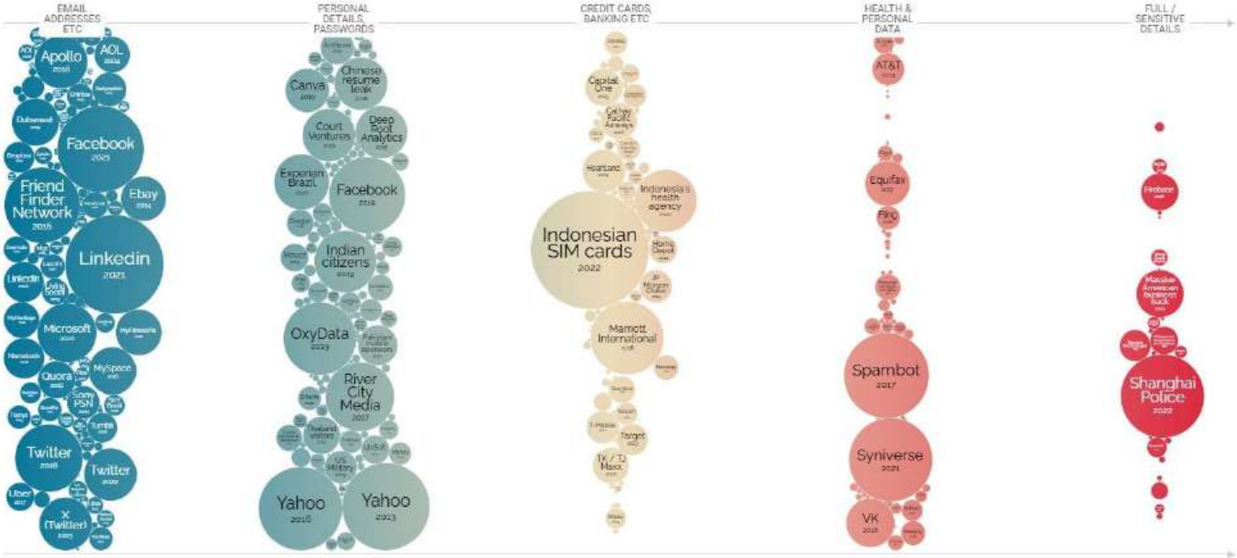
Uber Suffers New Data Leak After Third-Party Vendor Gets Hacked

December 12, 2022 By Heinrich Long — 4 Comments

A large collection of internal data was dumped over the weekend on a hacking forum and now Uber has confirmed a new data leak to RestorePrivacy that is unrelated to the September breach. Uber is blaming a third-party vendor. We analyzed the data for this report.

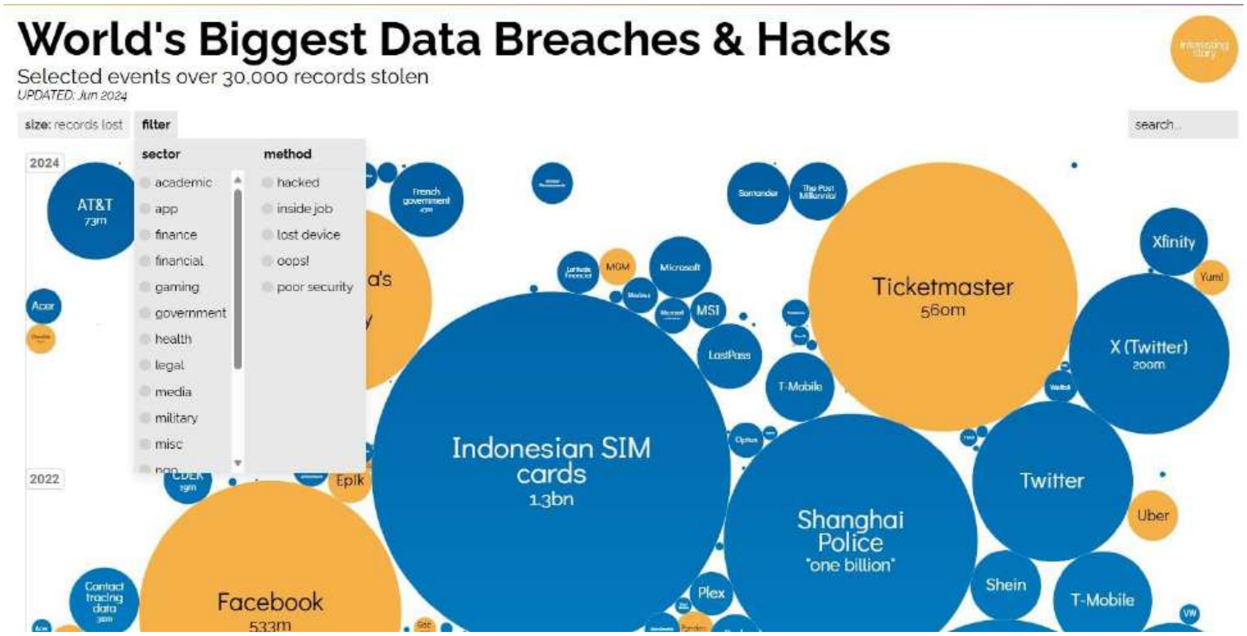
Update: Uber has now confirmed to RestorePrivacy that Teqtivity was the third-party vendor that was

7. Click the Data Sensitivity button on the World's Biggest Data Breaches & Hacks page. Note the color legend from Low to High that indicates how sensitive the data was.



8. Click the Year button to return to the original screen.

9. Click the Filter button to display the filter menu.

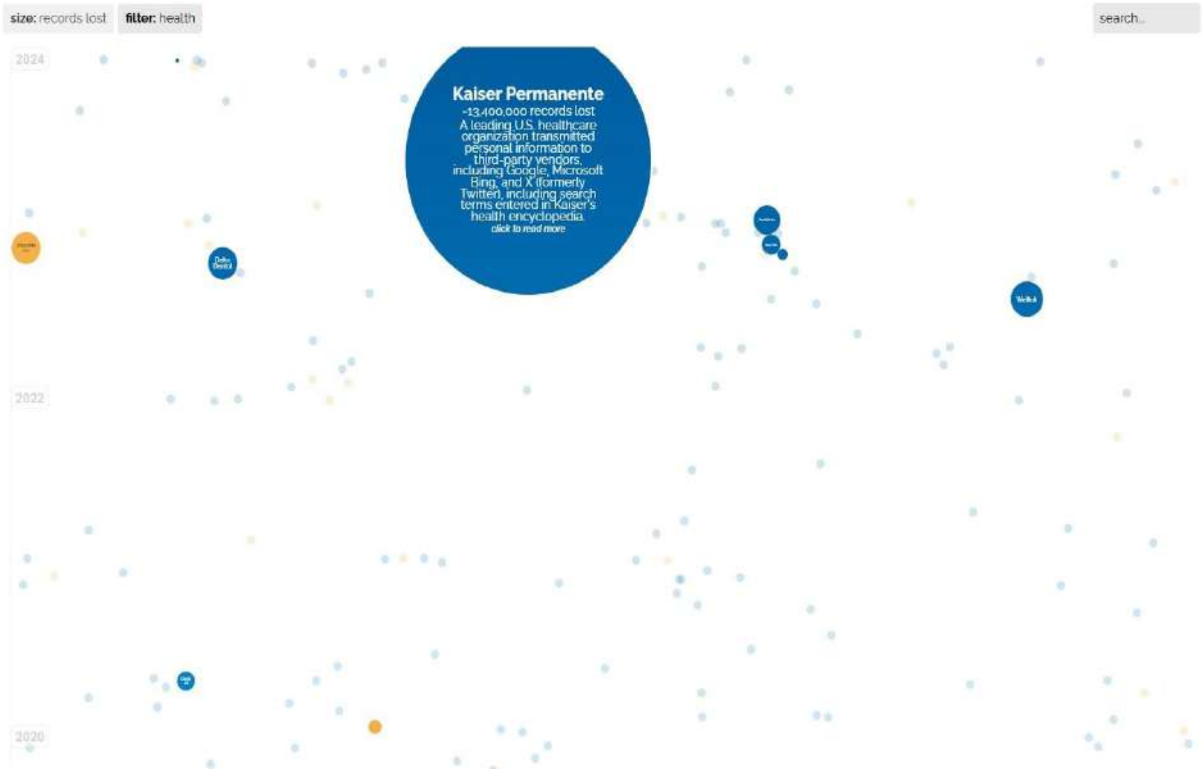


World's Biggest Data Breaches & Hacks

Selected events over 30,000 records stolen

UPDATED: Jun 2024

10. Under Sector, click healthcare to view those breaches related to the healthcare industry.



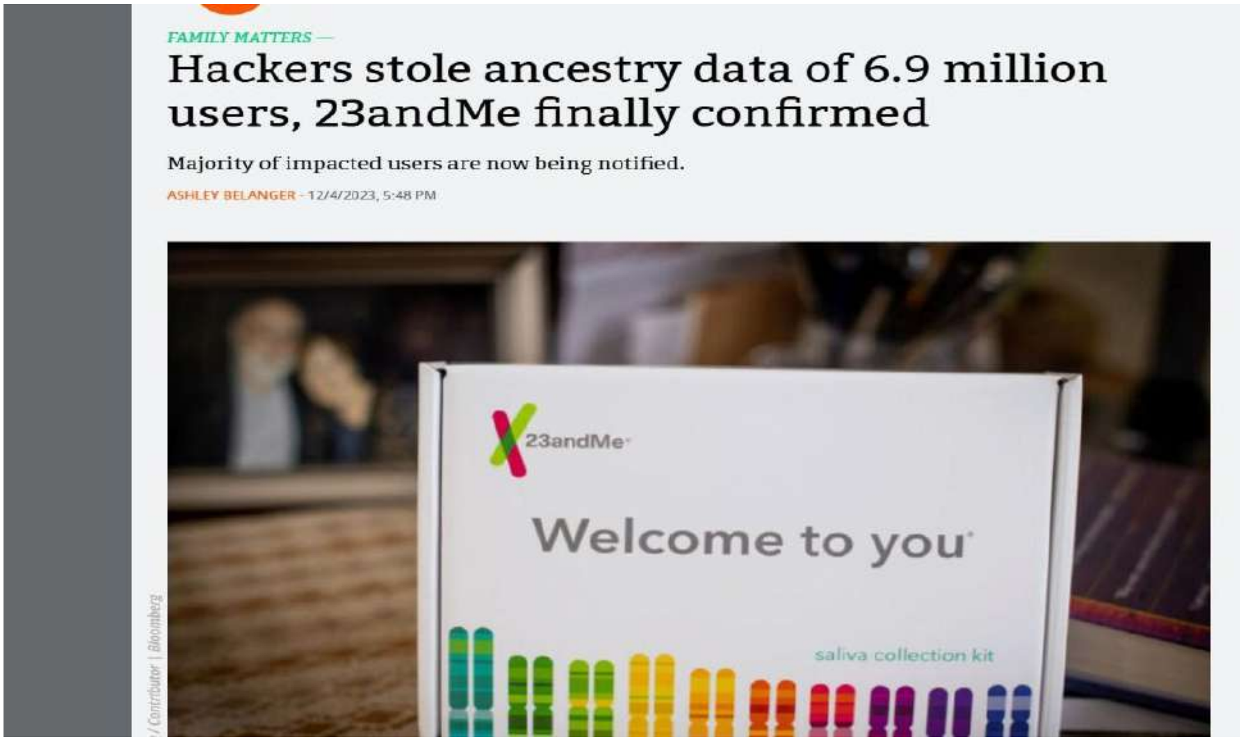
Kaiser Permanente

~13,400,000 records lost

A leading U.S. healthcare organization transmitted personal information to third-party vendors, including Google, Microsoft Bing, and X (formerly Twitter), including search terms entered in Kaiser's health encyclopedia.

click to read more

11. Click one of the bubbles and read the story.



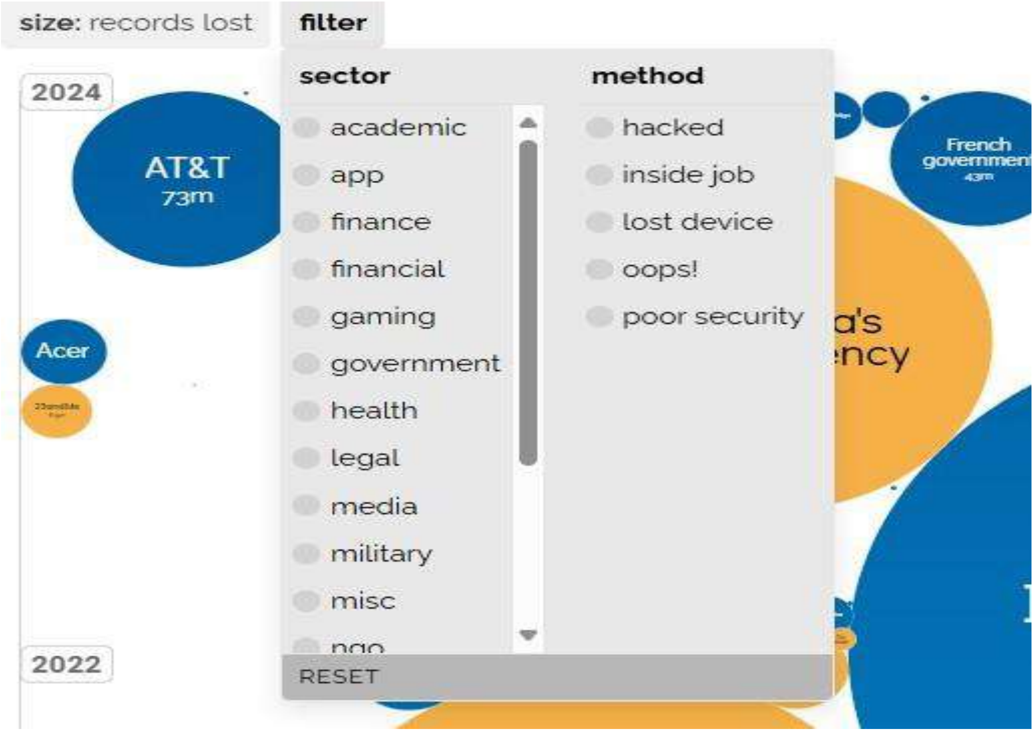
FAMILY MATTERS —

Hackers stole ancestry data of 6.9 million users, 23andMe finally confirmed

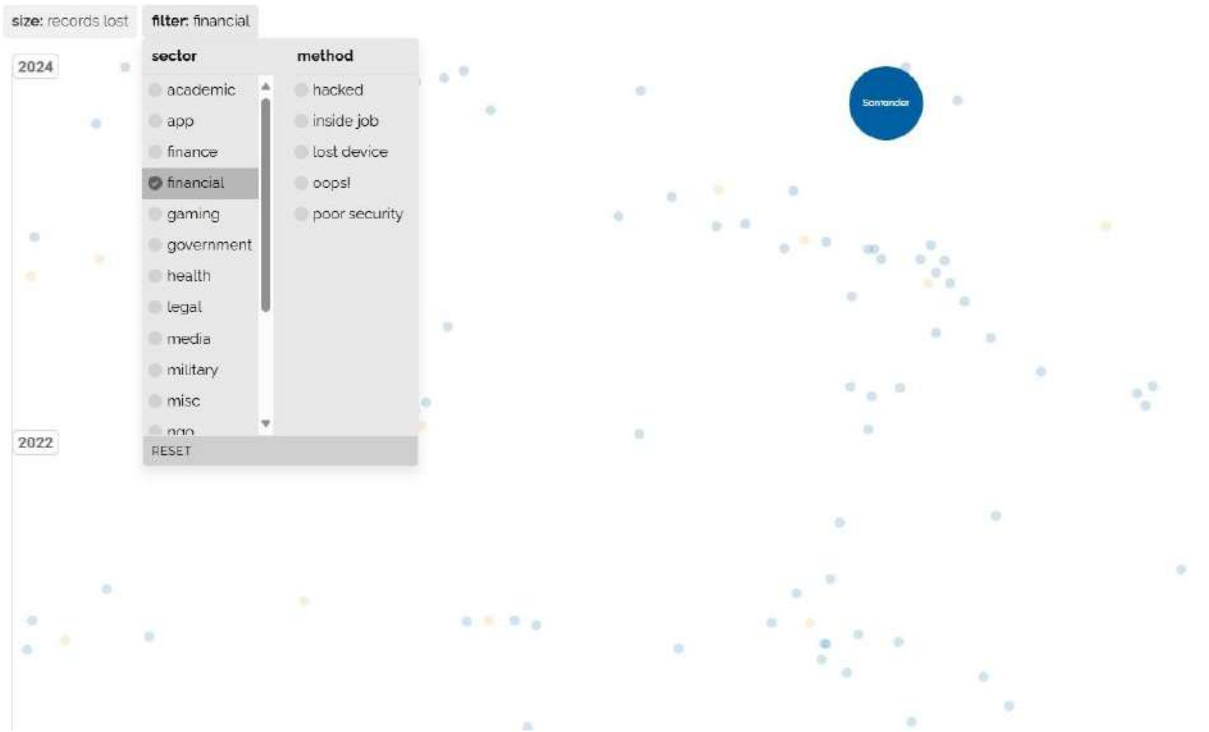
Majority of impacted users are now being notified.

ASHLEY BELANGER - 12/4/2023, 5:48 PM

12. Click Reset in the filter menu.

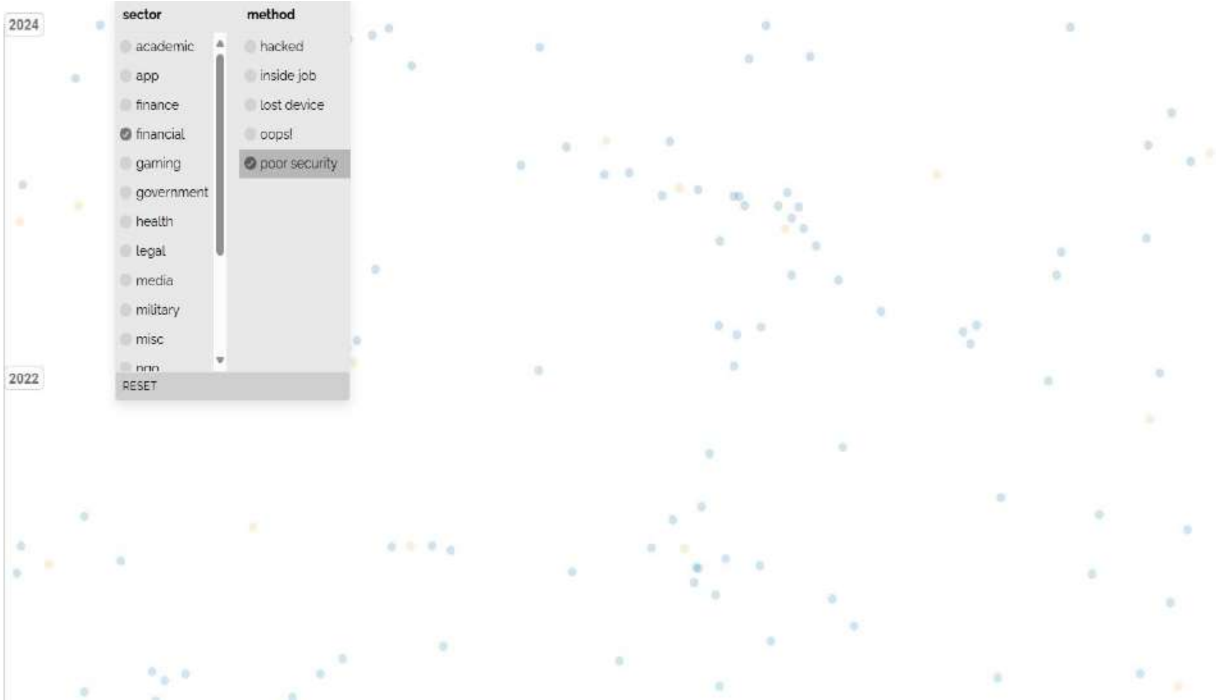


13. Select the sector financial.

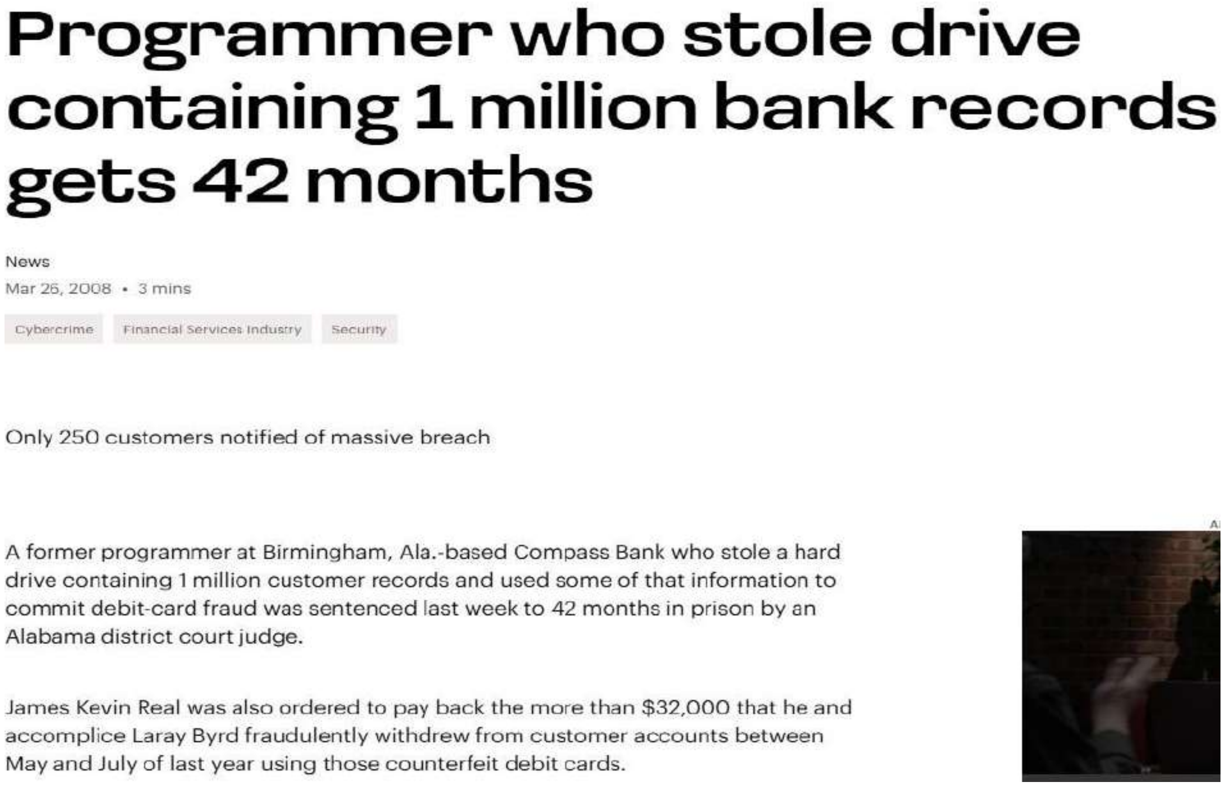

size: records lost

filter: financial

14. Select the method poor security.



15. Click one of the bubbles and read the story.



Programmer who stole drive containing 1 million bank records gets 42 months

News

Mar 26, 2008 • 3 mins

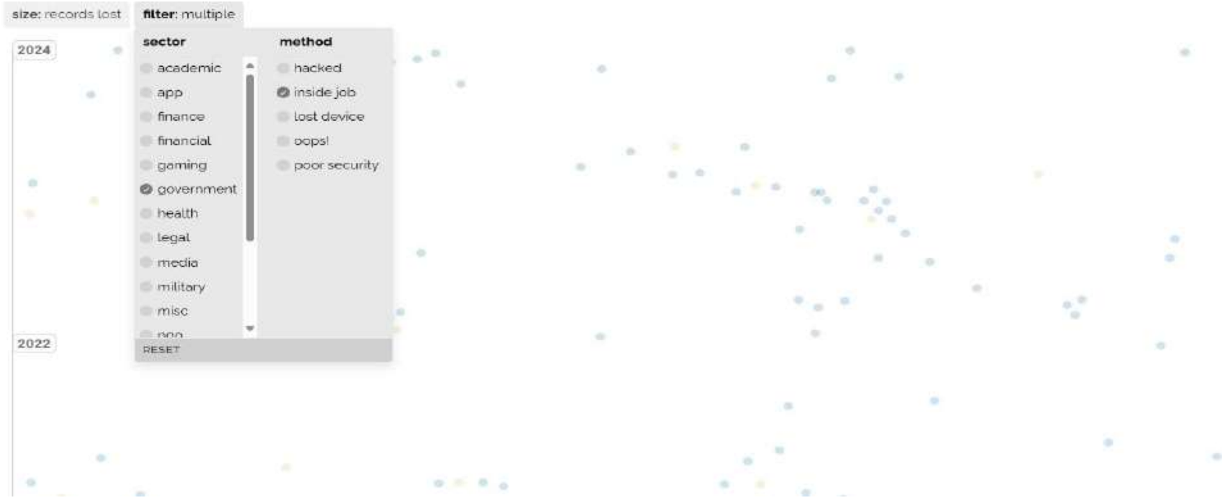
Cybercrime | Financial Services Industry | Security

Only 250 customers notified of massive breach

A former programmer at Birmingham, Ala.-based Compass Bank who stole a hard drive containing 1 million customer records and used some of that information to commit debit-card fraud was sentenced last week to 42 months in prison by an Alabama district court judge.

James Kevin Real was also ordered to pay back the more than $32,000 that he and accomplice Laray Byrd fraudulently withdrew from customer accounts between May and July of last year using those counterfeit debit cards.

16. Create your own filters to view different types of breaches. Does this graphic convey a compelling story of data breaches?



17. How does this visualization help you with the understanding of threats?

It helps you see what sectors/methods are most likely to be used for certain breaches, as well as the size of the breaches relative to the sector and data sensitivity.

18. Close all windows

References

Belanger, A. (2023, December 4). *Hackers stole ancestry data of 6.9 million users, 23andMe finally confirmed*. Ars Technica. https://arstechnica.com/tech-policy/2023/12/hackers-stole-ancestry-data-of-6-9-million-users-23andme-finally-confirmed/

Long, H. (2022, December 14). *Uber suffers new data leak after third-party vendor gets hacked*. RestorePrivacy. https://restoreprivacy.com/uber-data-leak-breach-third-party-vendor-hacked/

McCandless, D. (2022, June 1). *World's biggest data breaches & hacks*. Information is Beautiful. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Siddiqui, Z. (2023, October 5). *Casino giant MGM expects $100 million hit from Hack that led to data breach | reuters*. Casino giant MGM expects $100 million hit from hack that led to data breach. https://www.reuters.com/business/mgm-expects-cybersecurity-issue-negatively-impact-third-quarter-earnings-2023-10-05/

Vijayan, J. (2008, March 26). *Programmer who stole drive containing 1 million bank records gets 42 months*. Computerworld. https://www.computerworld.com/article/1570372/programmer-who-stole-drive-containing-1-million-bank-records-gets-42-months.html

Project 1-4: create a Virtual machine of Windows 10 for Security testing—Part 1

Objective: given a scenario, implement host or application security solutions.

Description: If you were unable to install the Windows Sandbox in Project 1-3, a different virtual machine can be created in which new applications can be installed or configuration settings changed without affecting the base computer. In a virtual machine environment, the “host” computer runs a “guest” operating system. Security programs and testing can be conducted within this guest operating system without affecting the regular host operating system. In this project, you create a virtual machine using oracle Virtualbox software.

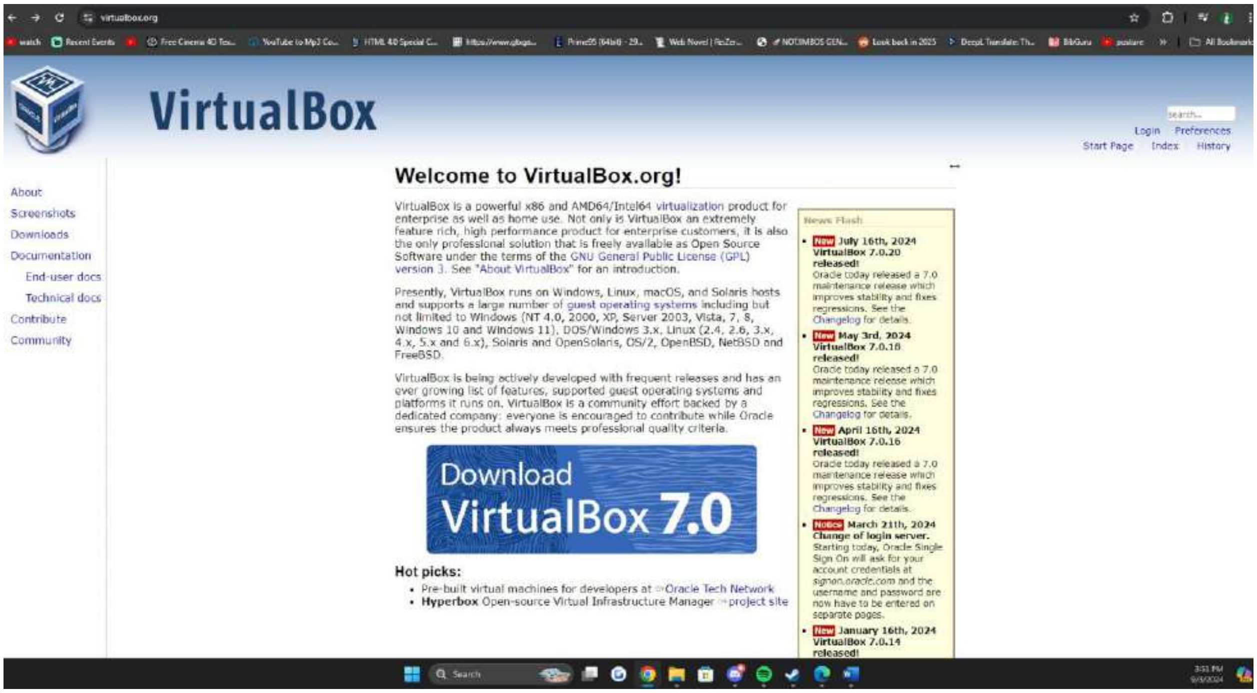
INTRODUCTION

VM or Virtual Machine’s are an act of isolating an operating system on your operating system. According to Scale Computing (2023),”VMs will enable you to create a virtual environment on your computer”[CITATION Sca23 \l 1033]. The act of using a Virtual Machine is a cost efficient and secure way to run things in that isolated sandbox. It works, according to Microsoft by creating a “virtual” version of a computer via virtualization and dedicating resources from your own machine to run it. It is also used to build and deploy apps on the cloud, trying out new operating system releases, accessing virus-infected data or running older applications, and more[CITATION Mic \l 1033].

---

1. Open a web browser and enter the urL www.virtualbox.org (If you are no longer able to access the site through this web address, use a search engine to search for “oracle Virtualbox download.”)

2. Click downloads (or a similar link or button).



Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, macOS, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, 7, 8, Windows 10 and Windows 11), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x, 4.x, 5.x and 6.x), Solaris and OpenSolaris, OS/2, OpenBSD, NetBSD and FreeBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Hot picks:

- Pre-built virtual machines for developers at Oracle Tech Network
- Hyperbox Open-source Virtual Infrastructure Manager project site

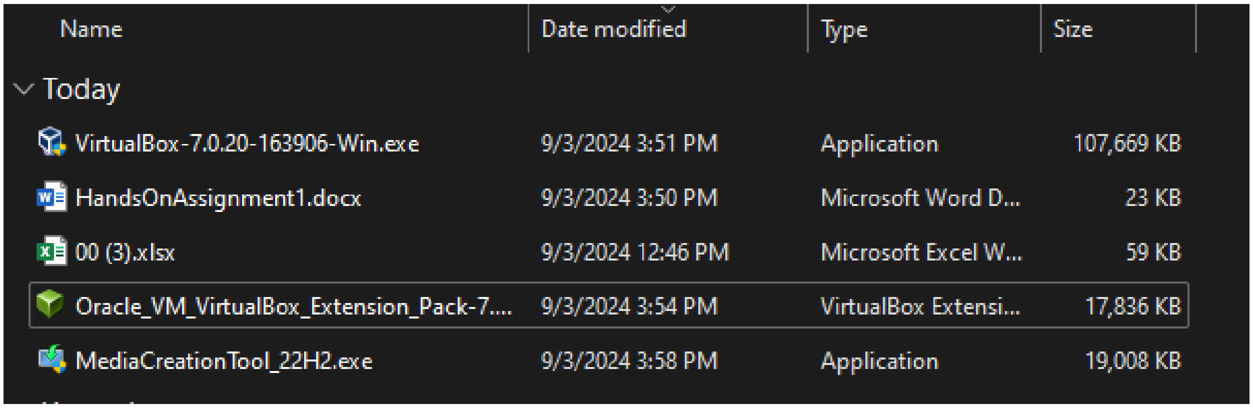
News Flash

- New July 16th, 2024 VirtualBox 7.0.20 released! Oracle today released a 7.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- New May 3rd, 2024 VirtualBox 7.0.18 released! Oracle today released a 7.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- New April 16th, 2024 VirtualBox 7.0.16 released! Oracle today released a 7.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- Notice March 21th, 2024 Change of login server. Starting today, Oracle Single Sign On will ask for your account credentials at signon.oracle.com and the username and password are now have to be entered on separate pages.
- New January 16th, 2024 VirtualBox 7.0.14 released!

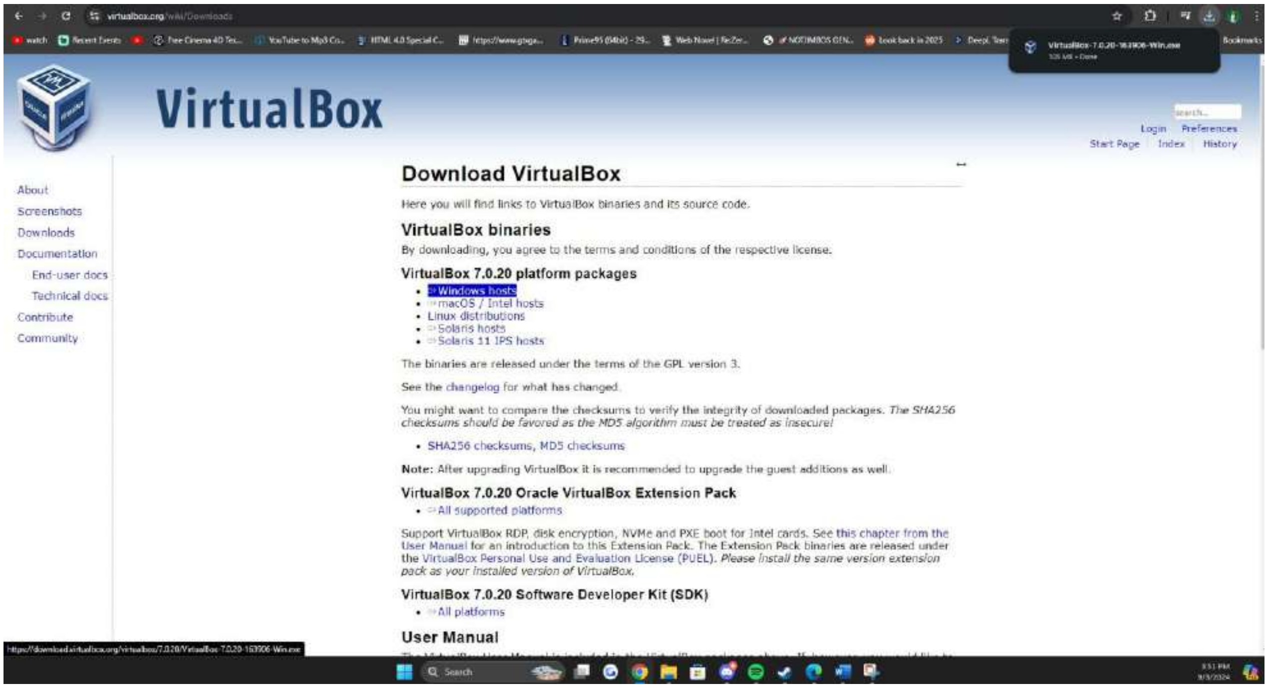
3. under Virtualbox binaries, select the latest version of Virtualbox to download for your specific host operating

system. For example, if you are running Windows, select the version for “Windows hosts.”

4. under Virtualbox x.x.x oracle VM Virtualbox extension Pack, click All supported platforms to download the extension package.



Name	Date modified	Type	Size
Today			
VirtualBox-7.0.20-163906-Win.exe	9/3/2024 3:51 PM	Application	107,669 KB
HandsOnAssignment1.docx	9/3/2024 3:50 PM	Microsoft Word D...	23 KB
00 (3).xlsx	9/3/2024 12:46 PM	Microsoft Excel W...	59 KB
Oracle_VM_VirtualBox_Extension_Pack-7....	9/3/2024 3:54 PM	VirtualBox Extensi...	17,836 KB
MediaCreationTool_22H2.exe	9/3/2024 3:58 PM	Application	19,008 KB



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

VirtualBox 7.0.20 platform packages

- Windows hosts
- macOS / Intel hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 7.0.20 Oracle VirtualBox Extension Pack

- All supported platforms

Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

VirtualBox 7.0.20 Software Developer Kit (SDK)

- All platforms

User Manual

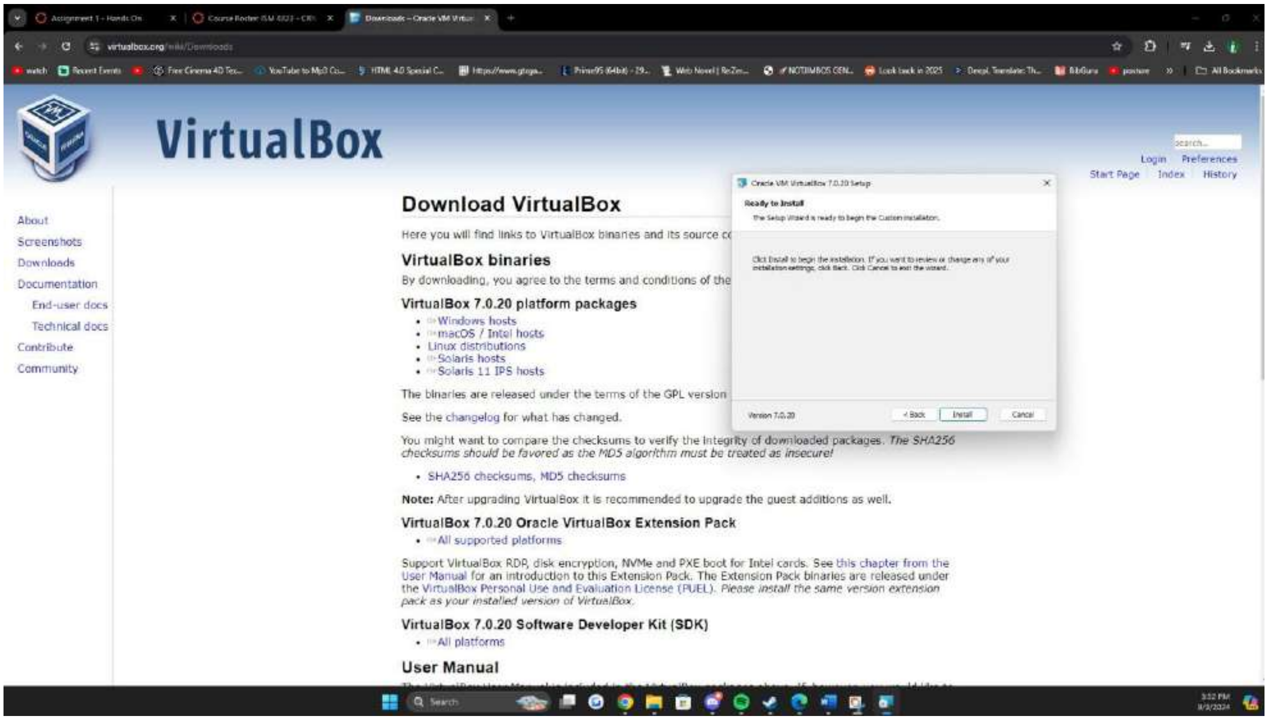
5. navigate to the folder that contains the downloads and launch the Virtualbox installation program VirtualBox

xxx-nnnnn-hhh.exe.

6. accept the default configurations from the installation wizard to install the program.

7. If you are asked “Would you like to install this device software?” on one or more occasions, click Install.

8. When completed, click Finish to launch Virtualbox.



Download VirtualBox

Here you will find links to VirtualBox binaries and its source co

VirtualBox binaries

By downloading, you agree to the terms and conditions of the

VirtualBox 7.0.20 platform packages

- Windows hosts
- macOS / Intel hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 7.0.20 Oracle VirtualBox Extension Pack

- All supported platforms

Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this chapter from the User Manual for an introduction to this Extension Pack. The Extension Pack binaries are released under the VirtualBox Personal Use and Evaluation License (PUEL). *Please install the same version extension pack as your installed version of VirtualBox.*

VirtualBox 7.0.20 Software Developer Kit (SDK)

- All platforms

User Manual

Oracle VM VirtualBox 7.0.20 Setup

Ready to Install

The Setup Wizard is ready to begin the Custom installation.

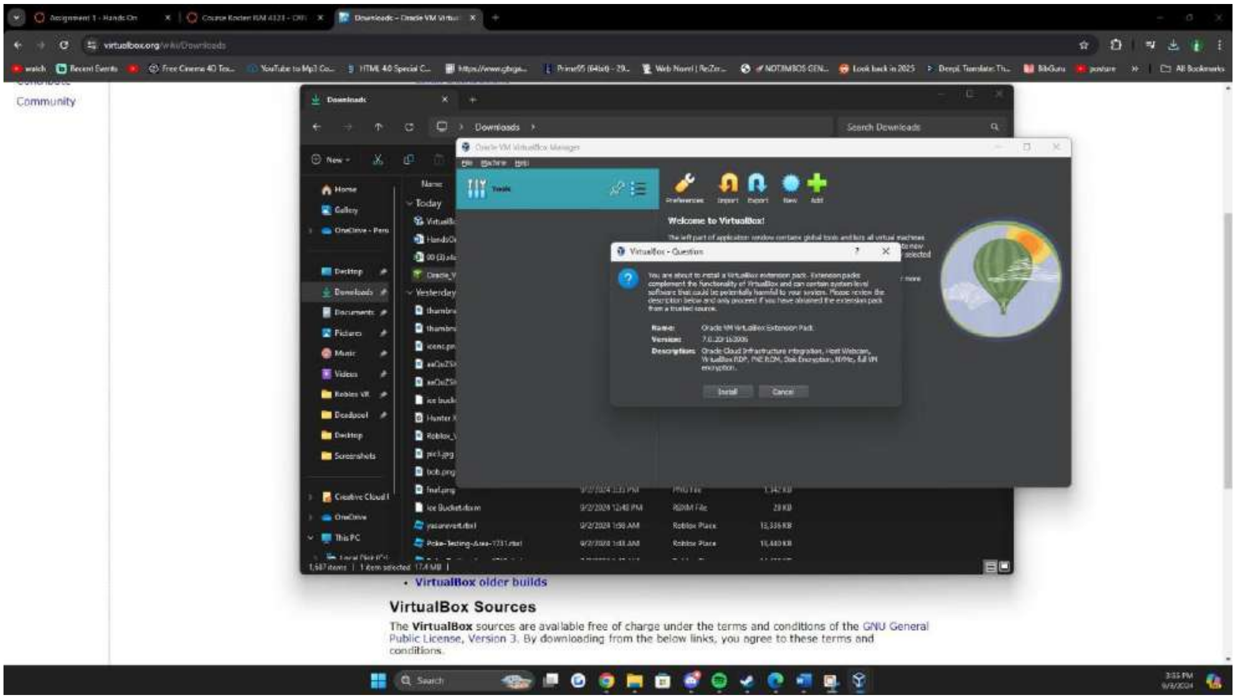
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Version 7.0.20

9. now install the Virtualbox extensions. click File and then click Preferences.

10. click extensions.

11. click the Add a package icon on the right side of the screen.



Welcome to VirtualBox!

VirtualBox - Question

You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.

Name: Oracle VM VirtualBox Extension Pack

Version: 7.0.20r163906

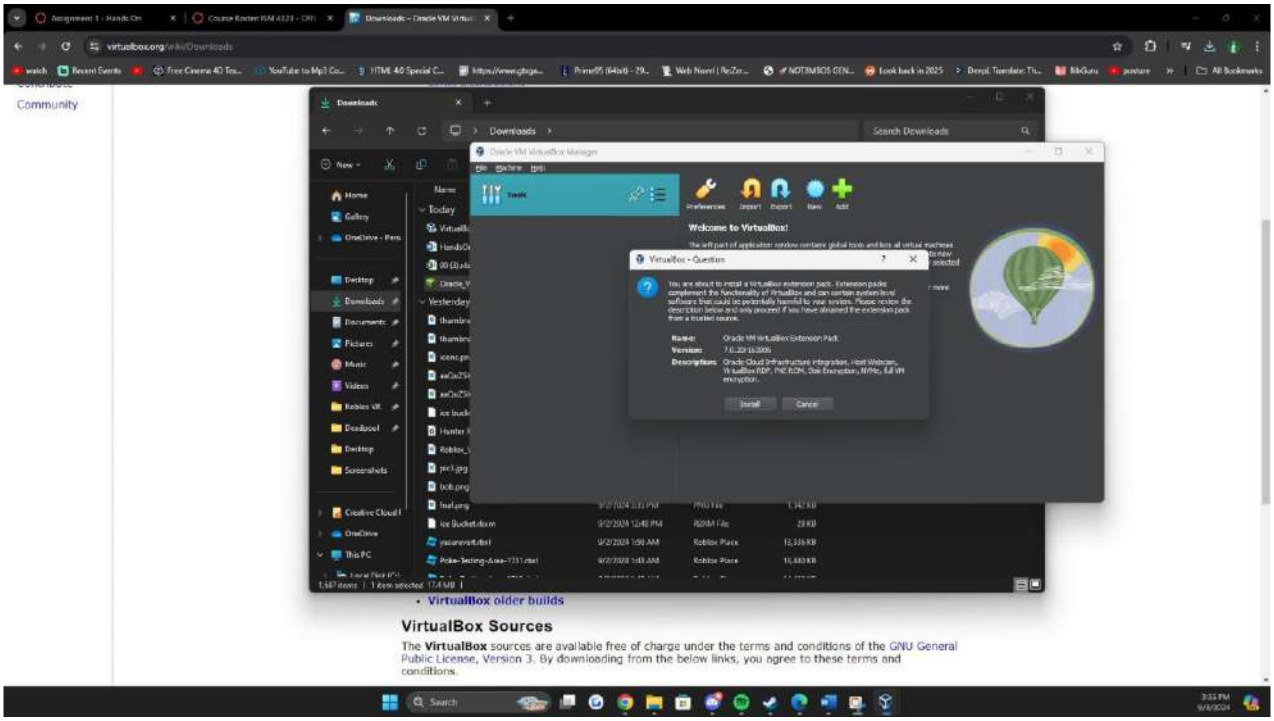
Description: Oracle Cloud Infrastructure integration, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe, full VM encryption.

- VirtualBox older builds

VirtualBox Sources

The **VirtualBox** sources are available free of charge under the terms and conditions of the GNU General Public License, Version 3. By downloading from the below links, you agree to these terms and conditions.

12. navigate to the folder that contains the extension pack downloaded earlier to select that file. click open.



VirtualBox - Question

You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.

Name: Oracle VM VirtualBox Extension Pack
Version: 7.0.20r163906
Description: Oracle Cloud Infrastructure integration, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe, full VM encryption.

Install Cancel

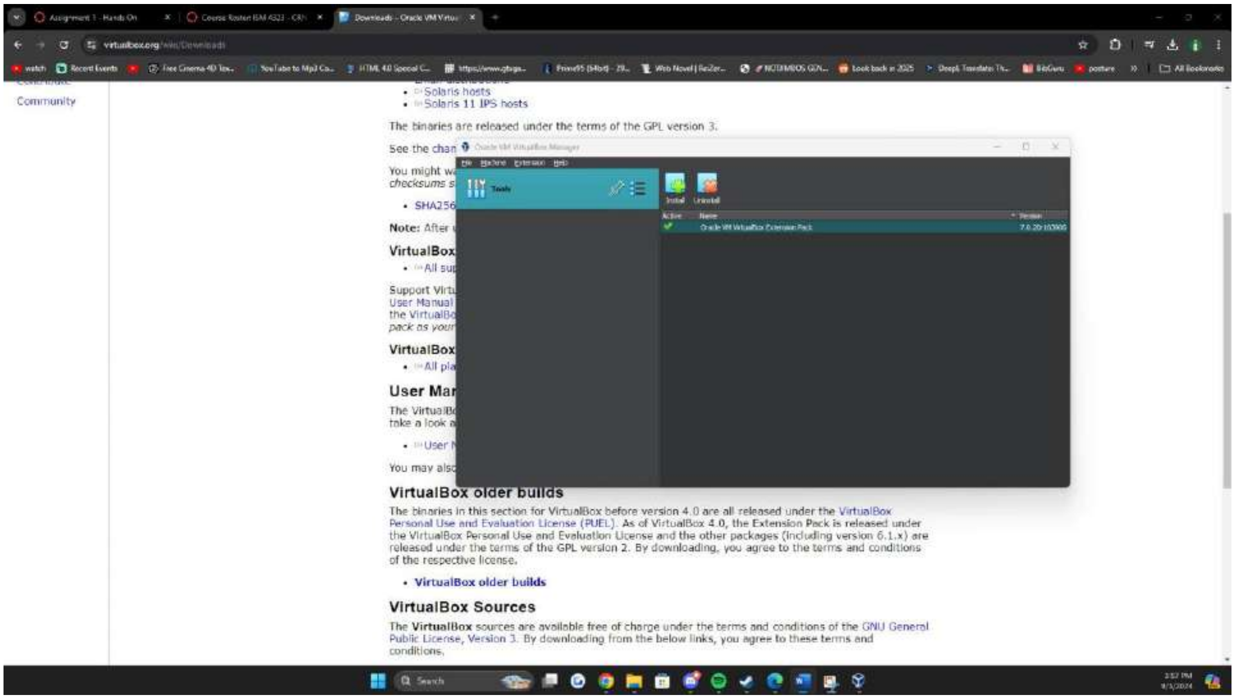
- VirtualBox older builds

VirtualBox Sources

The **VirtualBox** sources are available free of charge under the terms and conditions of the GNU General Public License, Version 3. By downloading from the below links, you agree to these terms and conditions.

13. click Install. Follow the necessary steps to complete the default installation.

14. remain in Virtualbox for the next project to configure Virtualbox and install the guest operating system.



Downloads – Oracle VM Virtua
virtualbox.org/wiki/Downloads
Community
Oracle VM VirtualBox Manager
File Machine Extension Help
Tools
Install
Uninstall
Active
Name
Version
Oracle VM VirtualBox Extension Pack
7.0.20r163906
Search

- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

See the chan

You might w
checksums s

- SHA256

Note: After

VirtualBox

- All sup

Support Virtu
User Manual
the VirtualBo
pack as your

VirtualBox

- All pla

User Mar

The VirtualB
take a look a

- User M

You may also

VirtualBox older builds

The binaries in this section for VirtualBox before version 4.0 are all released under the VirtualBox Personal Use and Evaluation License (PUEL). As of VirtualBox 4.0, the Extension Pack is released under the VirtualBox Personal Use and Evaluation License and the other packages (including version 6.1.x) are released under the terms of the GPL version 2. By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox older builds**

VirtualBox Sources

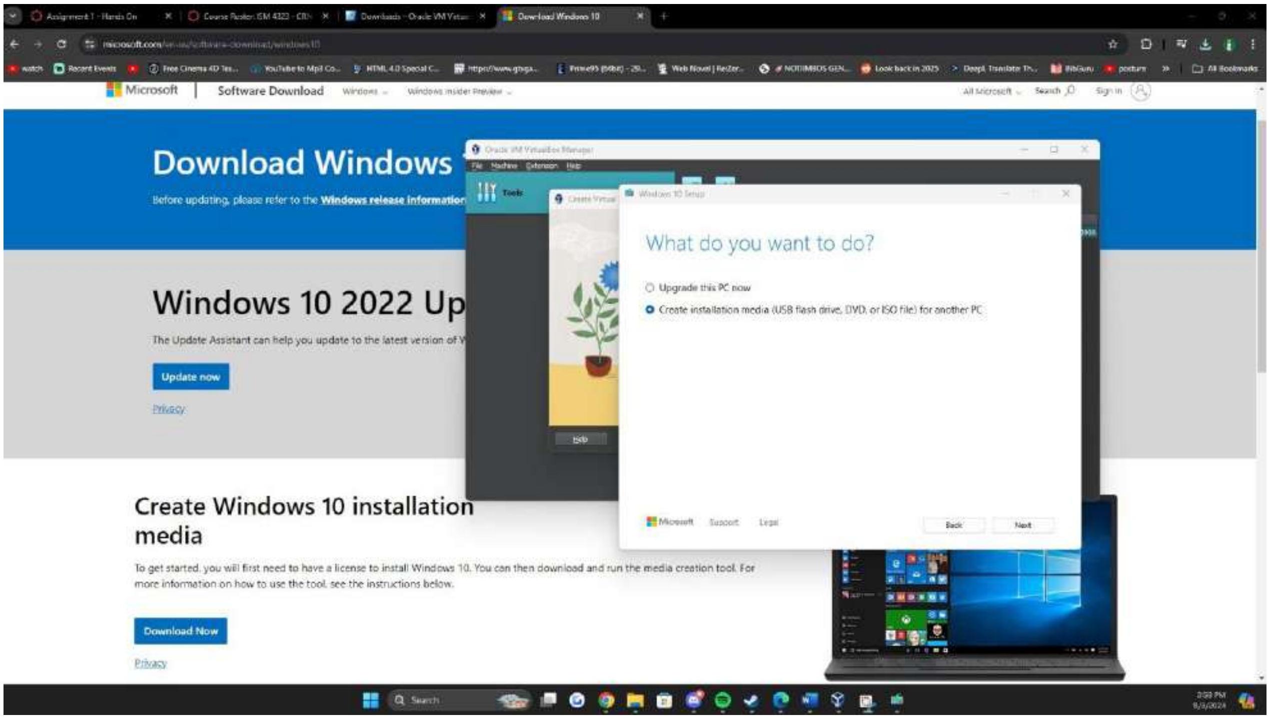
The **VirtualBox** sources are available free of charge under the terms and conditions of the GNU General Public License, Version 3. By downloading from the below links, you agree to these terms and conditions.

Project 1-5: create a Virtual machine of Windows 10 for Security testing—Part 2

Objective: Given a scenario, implement host or application security solutions.

Description: After installing Virtualbox, the next step is to create the guest operating system. For this project, Windows 10 will be installed. different options are available for obtaining a copy of Windows:

1. **obtain the ISo image of Windows 10 using one of the preceding options and save it on the hard drive of the computer.**



What do you want to do?

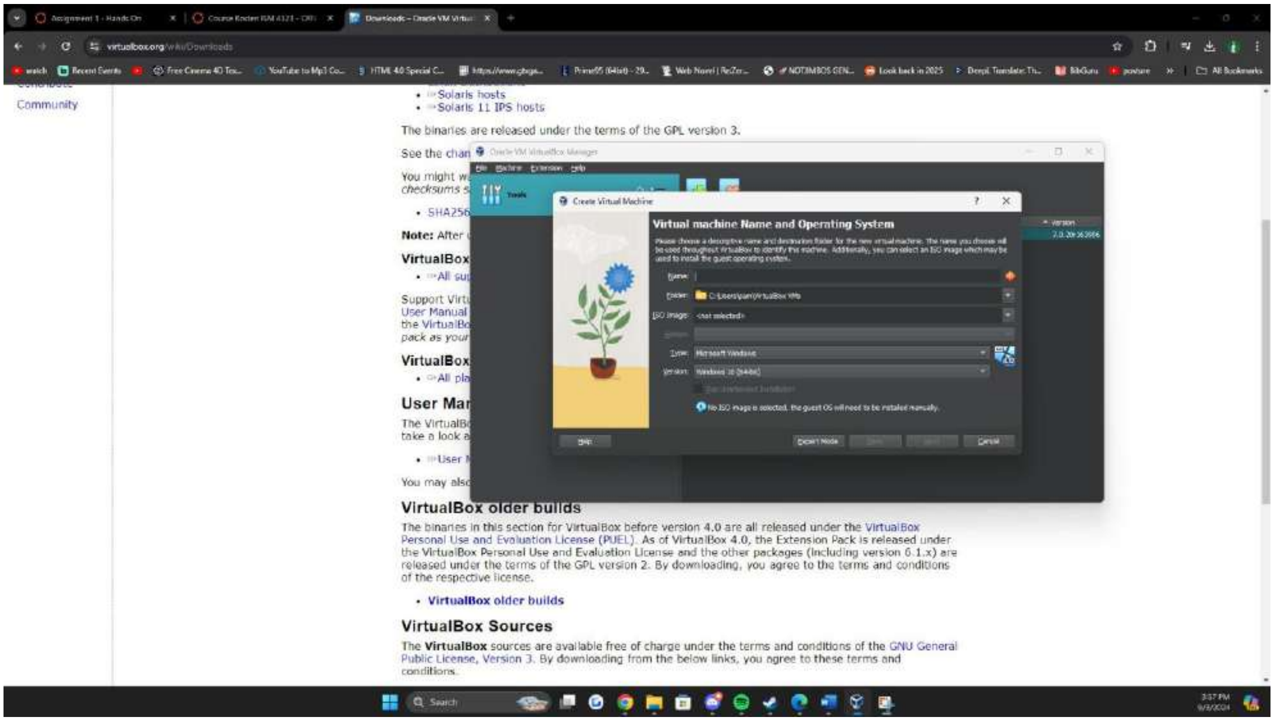
○ Upgrade this PC now

● Create installation media (USB flash drive, DVD, or ISO file) for another PC

To get started, you will first need to have a license to install Windows 10. You can then download and run the media creation tool. For more information on how to use the tool, see the instructions below.

2. **Launch Virtualbox.**

3. click New.



- Solaris hosts
- Solaris 11 IPS hosts

The binaries are released under the terms of the GPL version 3.

Create Virtual Machine

Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name:

Folder: C:\Users\pam\VirtualBox VMs

ISO Image: <not selected>

Type: Microsoft Windows

Version: Windows 10 (64-bit)

No ISO image is selected, the guest OS will need to be installed manually.

VirtualBox older builds

The binaries in this section for VirtualBox before version 4.0 are all released under the VirtualBox Personal Use and Evaluation License (PUEL). As of VirtualBox 4.0, the Extension Pack is released under the VirtualBox Personal Use and Evaluation License and the other packages (including version 6.1.x) are released under the terms of the GPL version 2. By downloading, you agree to the terms and conditions of the respective license.

- VirtualBox older builds

VirtualBox Sources

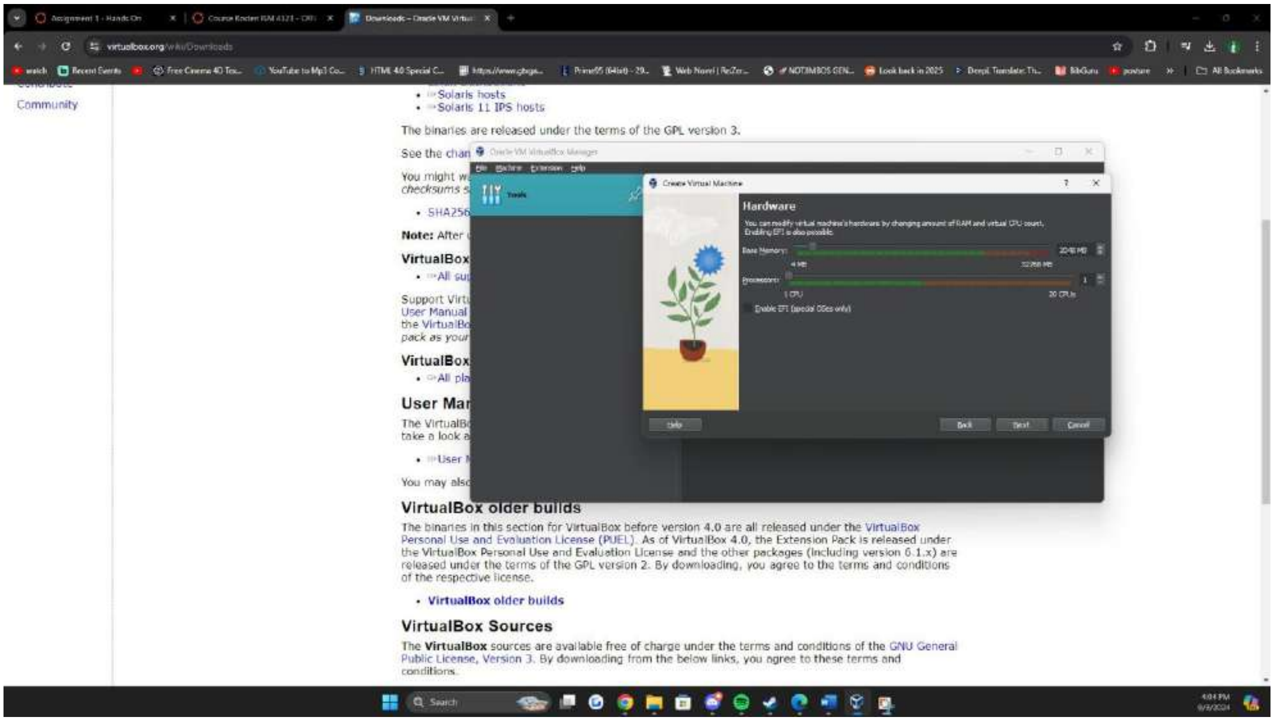
The **VirtualBox** sources are available free of charge under the terms and conditions of the GNU General Public License, Version 3. By downloading from the below links, you agree to these terms and conditions.

4. In the name: box, enter windows 10 as the name of the virtual machine.

5. be sure that the Type: box displays Microsoft windows and the Version: box changes to windows 10 (xx-bit).

click Next.

6. under Memory size, accept the recommended size or increase the allocation if you have sufficient raM on your computer. click Next.



Create Virtual Machine

Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB (4 MB – 32768 MB)

Processors: 1 (1 CPU – 20 CPUs)

□ Enable EFI (special OSes only)

The binaries are released under the terms of the GPL version 3.

VirtualBox older builds

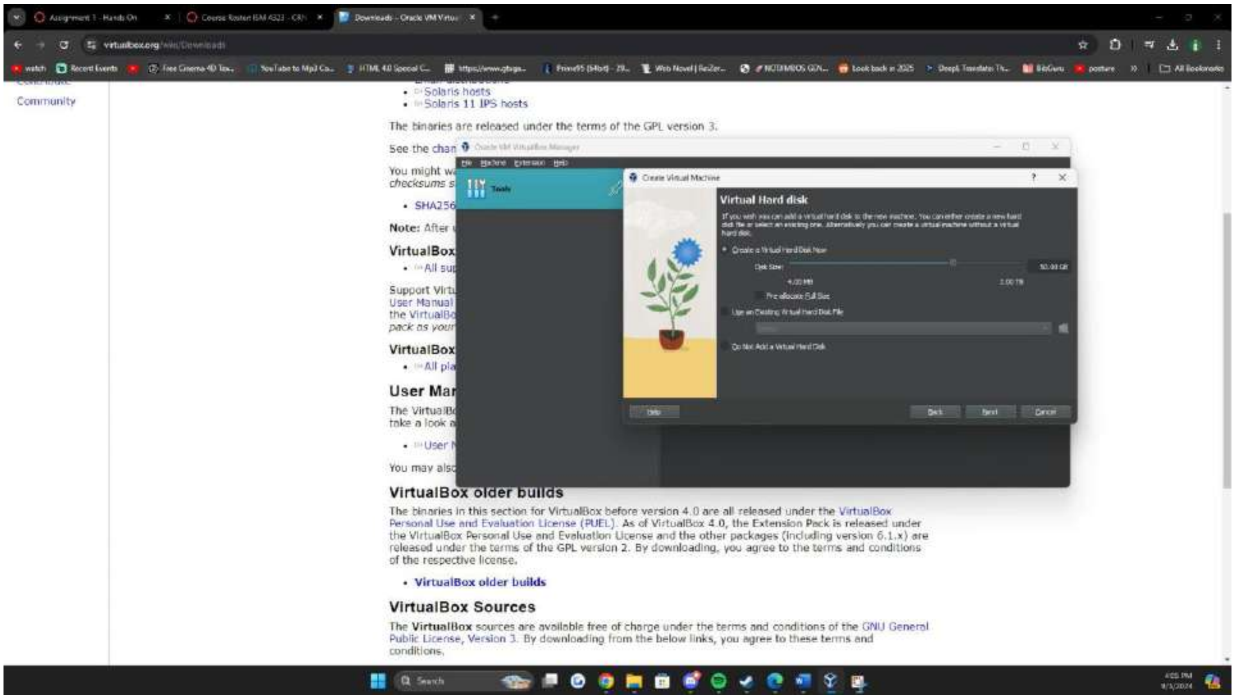
The binaries in this section for VirtualBox before version 4.0 are all released under the VirtualBox Personal Use and Evaluation License (PUEL). As of VirtualBox 4.0, the Extension Pack is released under the VirtualBox Personal Use and Evaluation License and the other packages (including version 6.1.x) are released under the terms of the GPL version 2. By downloading, you agree to the terms and conditions of the respective license.

- VirtualBox older builds

VirtualBox Sources

The **VirtualBox** sources are available free of charge under the terms and conditions of the GNU General Public License, Version 3. By downloading from the below links, you agree to these terms and conditions.

7. under hard disk, accept Create a virtual hard drive now. click Create.



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 50.00 GB (4.00 MB – 2.00 TB)

□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

○ Do Not Add a Virtual Hard Disk

The binaries are released under the terms of the GPL version 3.

VirtualBox older builds

The binaries in this section for VirtualBox before version 4.0 are all released under the VirtualBox Personal Use and Evaluation License (PUEL). As of VirtualBox 4.0, the Extension Pack is released under the VirtualBox Personal Use and Evaluation License and the other packages (including version 6.1.x) are released under the terms of the GPL version 2. By downloading, you agree to the terms and conditions of the respective license.

- VirtualBox older builds

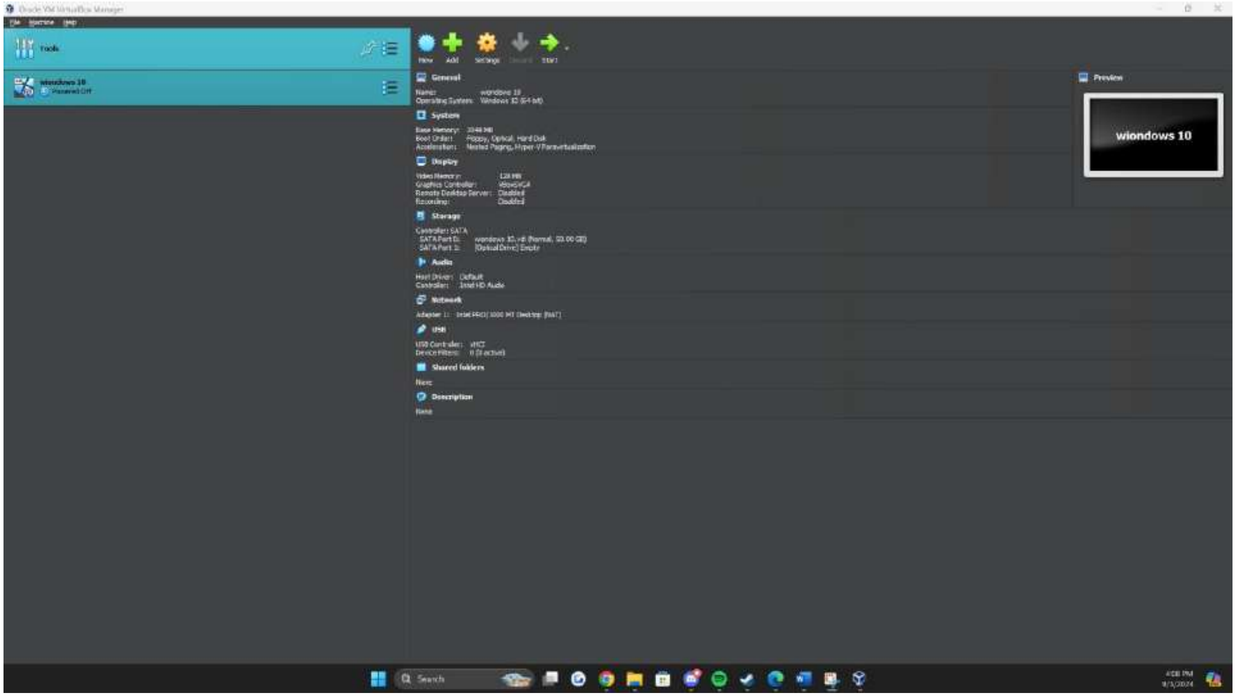
VirtualBox Sources

The **VirtualBox** sources are available free of charge under the terms and conditions of the GNU General Public License, Version 3. By downloading from the below links, you agree to these terms and conditions.

8. under hard drive file type, accept the default VId (VirtualBox disk Image). click Next.

9. under Storage on physical hard drive, accept the default dynamically allocated. click Next.

10. under File location and size, accept windows 10. click Create.



General

Name: wiondows 10
Operating System: Windows 10 (64-bit)

System

Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: wiondows 10.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: xHCI
Device Filters: 0 (0 active)

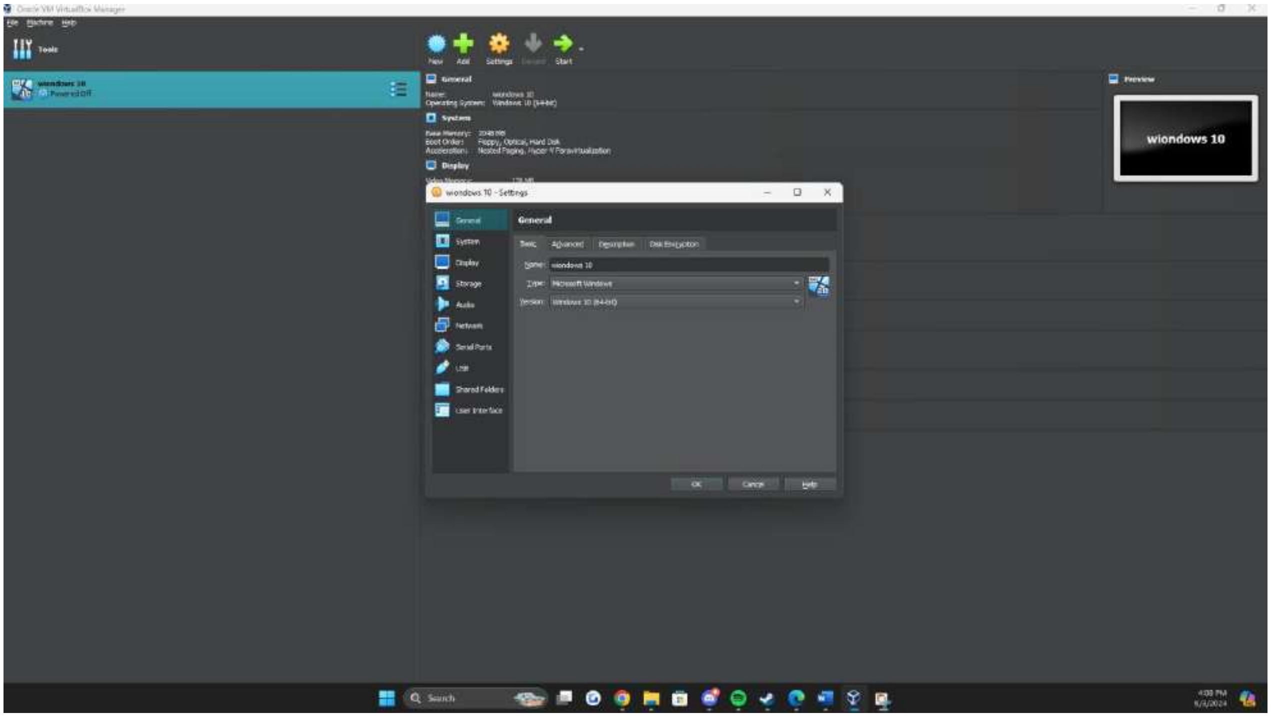
Shared folders

None

Description

None

11. now the configuration settings for the virtual machine are set. next you will load the Windows 10 ISO image. click Settings.



General
Name: wiondows 10
Operating System: Windows 10 (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 128 MB

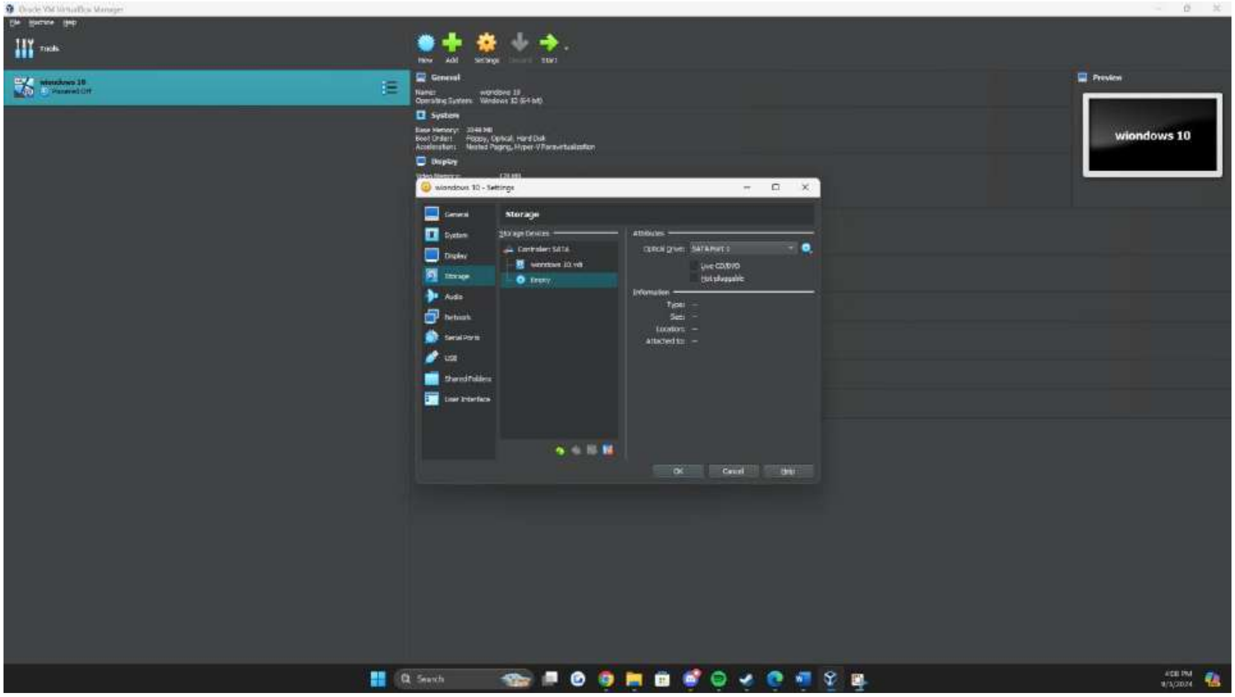
wiondows 10 - Settings

General

Name: wiondows 10
Type: Microsoft Windows
Version: Windows 10 (64-bit)

12. In the left pane, click Storage.

13. under controller: click empty.



General
Name: wiondows 10
Operating System: Windows 10 (64-bit)

System
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display
Video Memory: 128 MB

wiondows 10 - Settings

Storage

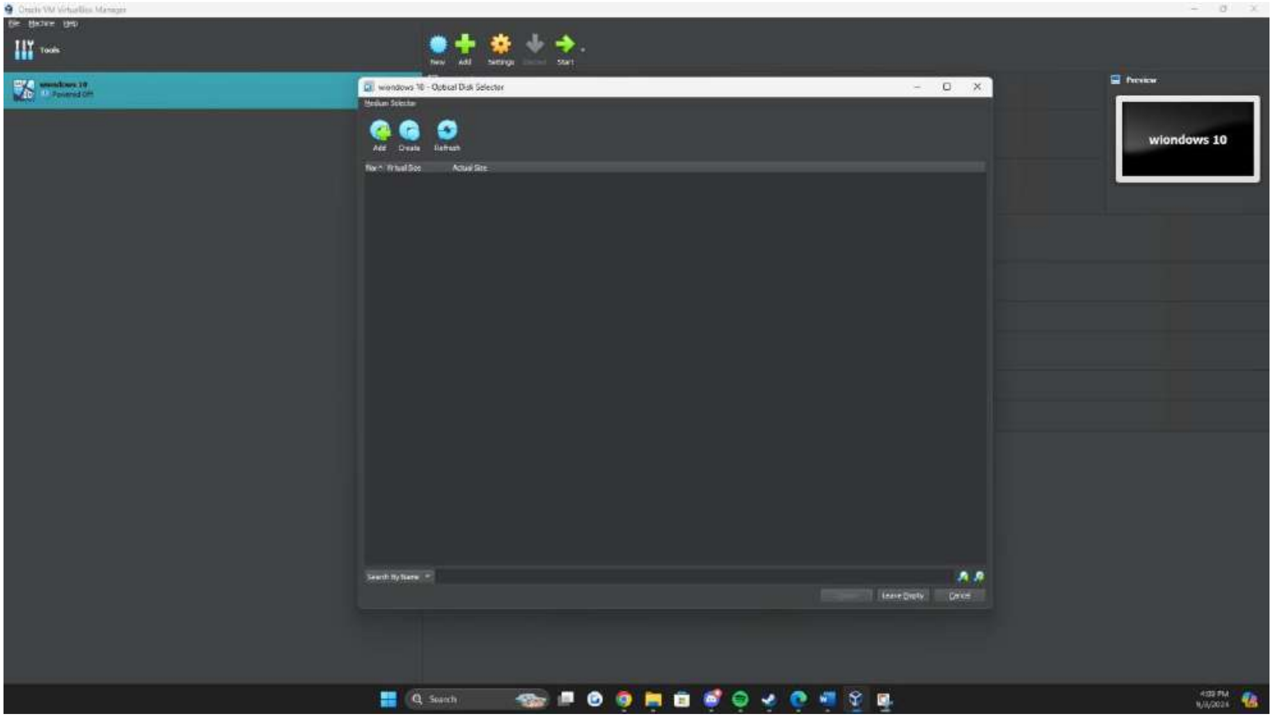
Storage Devices
Controller: SATA
wiondows 10.vdi
Empty

Attributes
Optical Drive: SATA Port 1
□ Live CD/DVD
□ Hot-pluggable

Information
Type: --
Size: --
Location: --
Attached to: --

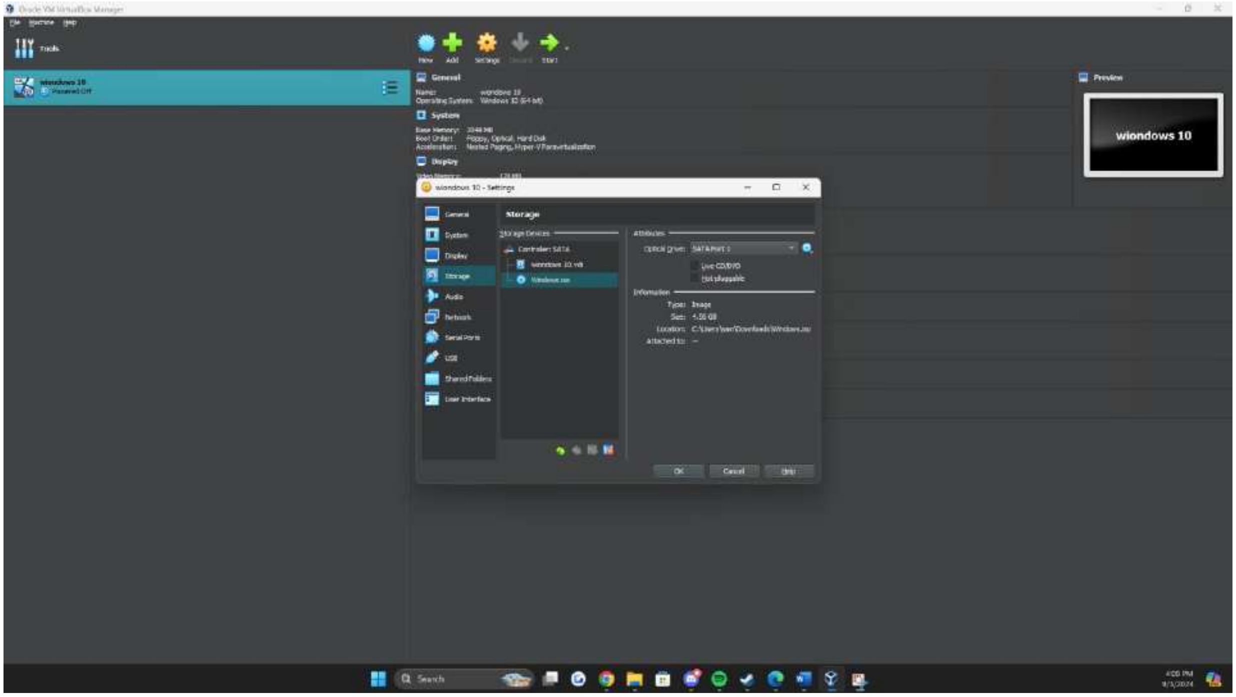
14. In the right page under attributes, click the icon of the optical disc.

15. click Choose Virtual optical disk File.



16. navigate to the location of the Windows 10 ISo file and click open.

17. click ok.



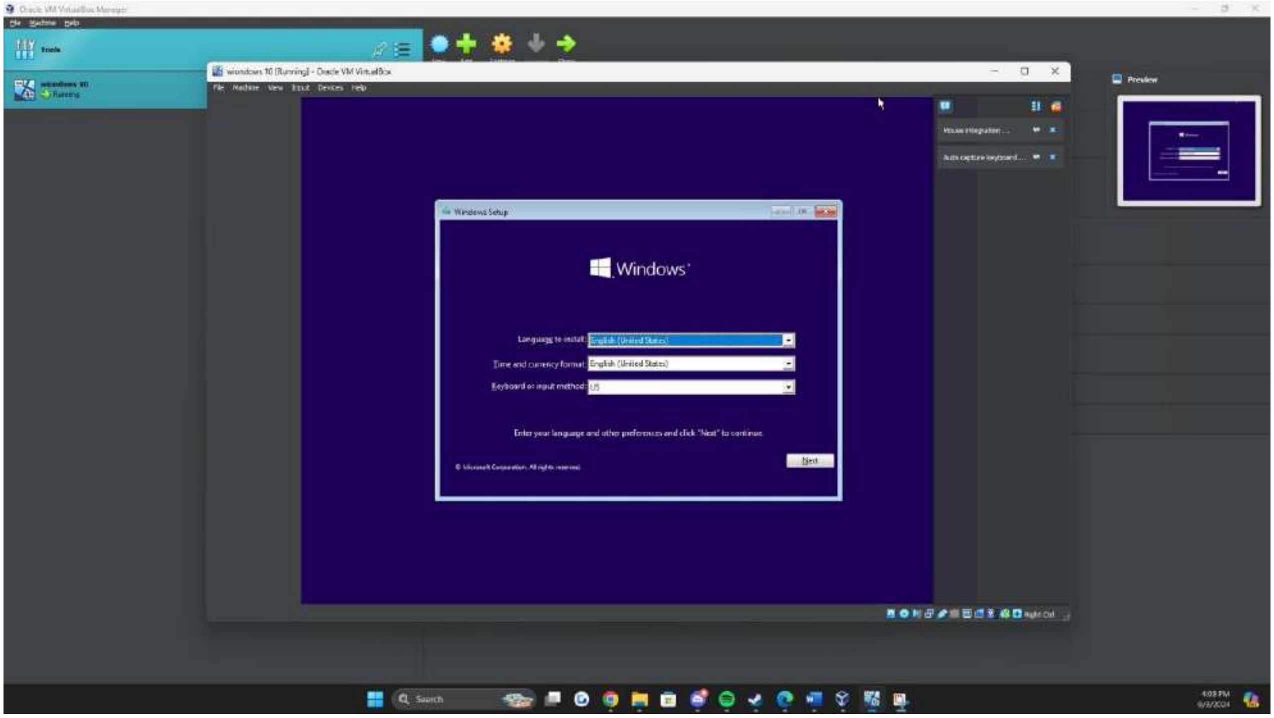
Name: wiondows 10
Operating System: Windows 10 (64-bit)
Base Memory: 2048 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Controller: SATA
wiondows 10.vdi
Windows.iso

Optical Drive: SATA Port 1
□ Live CD/DVD
□ Hot-pluggable

Type: Image
Size: 4.55 GB
Location: C:\Users\wan\Downloads\Windows.iso
Attached to: --

18. click Start to launch the Windows 10 ISo.



Windows Setup

Language to install: English (United States)

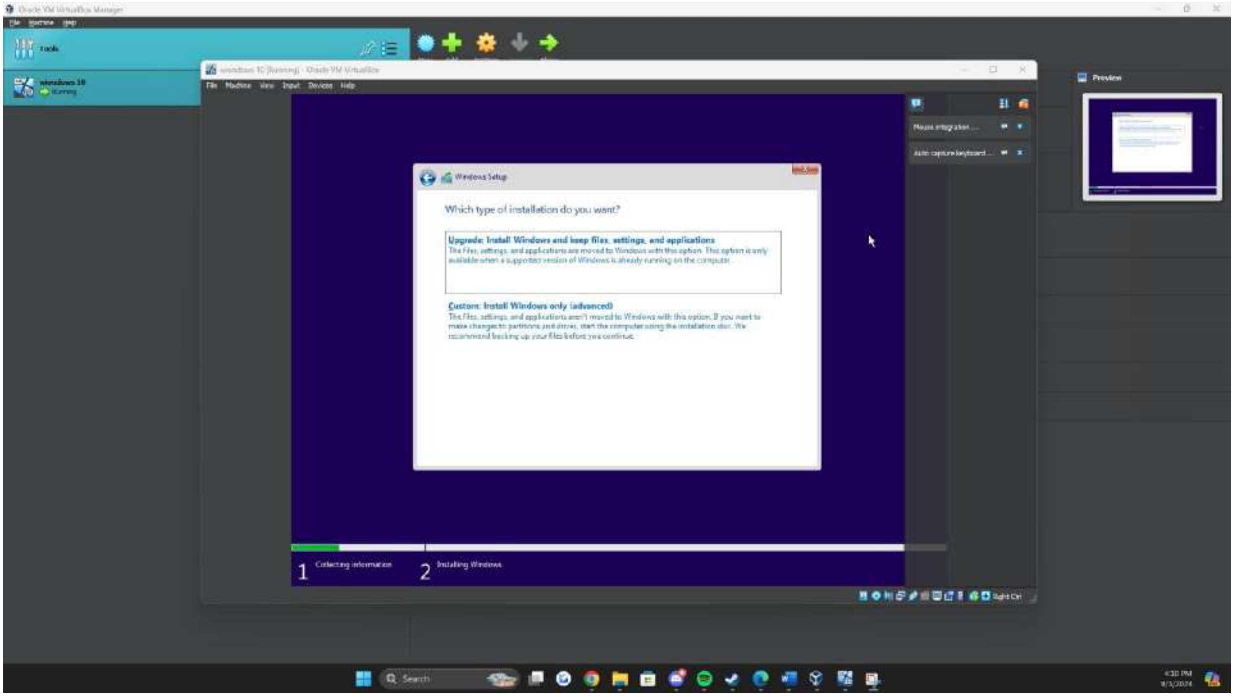
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© Microsoft Corporation. All rights reserved.

19. Follow the Windows 10 installation wizard to complete the installation.



Windows Setup

Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

20. **To close the Windows 10 guest operating system in Virtualbox, click File and then click exit.**

21. **close all windows.**

References

Microsoft. (n.d.). *What is a virtual machine (VM)?* Retrieved from Microsoft: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine

Scale Computing. (2023, September 25). *Understanding Virtual Machine Advantages and Disadvantages*. Retrieved from Scale Computing: https://www.scalecomputing.com/resources/understanding-virtual-machine-advantages-and-disadvantages

Project 2-1: Exploring Common Vulnerabilities and Exposures (Bonus)

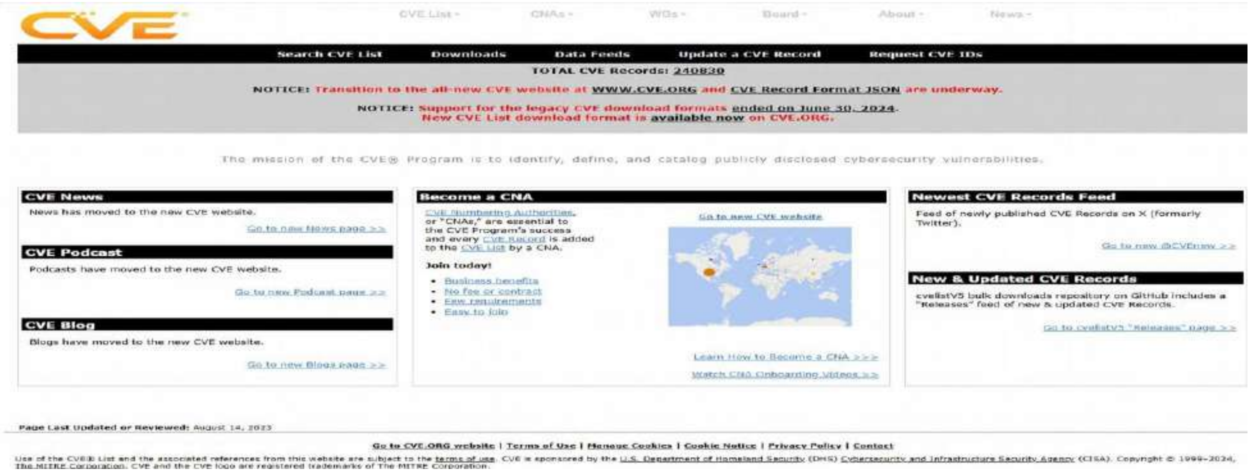
Objective: Summarize the techniques used in security assessments.

Description: Vulnerability feeds are available to provide updated information to scanning software about the latest vulnerabilities. One of the most highly regarded vulnerability feeds is the Mitre Common Vulnerabilities and Exposures (CVE). Feeds can also be manually examined for information on the latest vulnerabilities. In this project, you will learn more about CVE and view CVE information.

Introduction:

Vulnerabilities are a common reality for anyone in cybersecurity. The CVE allows anyone to monitor what these vulnerabilities are, when they occurred, and their severity, as well as the organization they occurred in. The monitoring and communication of this information can be essential in keeping everything safe and making sure vulnerabilities are patched promptly.

1. Open your web browser and enter the URL https://cve.mitre.org/ (if you are no longer able to access the site through this web address, use a search engine to search for “Mitre CVE”).



TOTAL CVE Records: 240830

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.
New CVE List download format is available now on CVE.ORG.

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE News

News has moved to the new CVE website.

Go to new News page >>

CVE Podcast

Podcasts have moved to the new CVE website.

Go to new Podcast page >>

CVE Blog

Blogs have moved to the new CVE website.

Go to new Blogs page >>

Become a CNA

CVE Numbering Authorities, or "CNAs," are essential to the CVE Program's success and every CVE Record is added to the CVE List by a CNA.

Join today!

- Business benefits
- No fee or contract
- Few requirements
- Easy to join

Go to new CVE website

Learn How to Become a CNA >>>

Watch CNA Onboarding Videos >>

Newest CVE Records Feed

Feed of newly published CVE Records on X (formerly Twitter).

Go to new @CVEnew >>

New & Updated CVE Records

cvelistV5 bulk downloads repository on GitHub includes a "Releases" feed of new & updated CVE Records.

Go to cvelistV5 "Releases" page >>

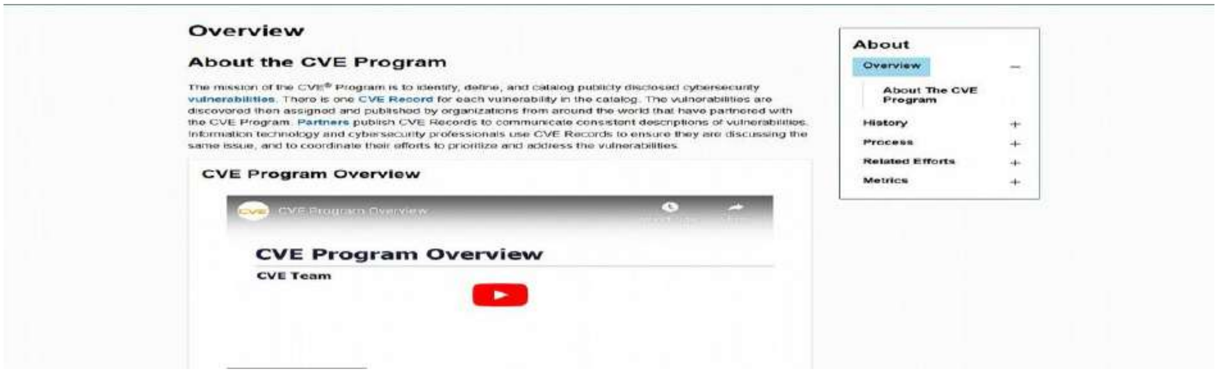
Page Last Updated or Reviewed: August 14, 2023

Go to CVE.ORG website | Terms of Use | Manage Cookies | Cookie Notice | Privacy Policy | Contact

Use of the CVE® List and the associated references from this website are subject to the terms of use. CVE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2024, The MITRE Corporation. CVE and the CVE logo are registered trademarks of The MITRE Corporation.

2. Click About.

3. Click About CVE.



Overview

About the CVE Program

The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

CVE Program Overview

CVE Program Overview

CVE Team

4. This page gives a brief overview of CVE. Read through the information regarding CVE. In your own words, how would you describe it? How does it work? What advantages does it provide?

It identifies, catalogs, and defines cybersecurity vulnerabilities. When vulnerabilities are discovered, they are assigned and published by organizations around the world that have partnered with the program. These vulnerabilities can then be used to communicate consistent descriptions of vulnerabilities which can be used to coordinate efforts addressing vulnerabilities

5. Point to About.

6. Click FAQs to display more detailed information on CVE. Who is behind CVE? Who owns it? How is it used? How does CVE compare to a vulnerability database? How would you answer the argument that threat actors could use CVE?

It's owned by the “Mitre” corporation, which has been sponsored by a multitude of government agencies and is used to take in information and monitor vulnerabilities for agencies/companies. The CVE is very similar to the NVD and other vulnerability databases, but from what I've gathered it has a more governmental focus. I would say it's a valid argument that threat actors could use the CVE, which is why vulnerabilities should be posted a little bit after the agency/company has been notified of it. I also thinking having this posted promotes promptly fixing issues

7. Scroll down to CVE Entries. Describe the three elements that make up a CVE Entry

CVE Identifier (CVE-ID): This is a unique identifier assigned to the vulnerability or exposure. It usually follows a format like CVE-YYYY-NNNNN, where "YYYY" represents the year, the vulnerability was disclosed or assigned, and "NNNNN" is a sequential number. For example, CVE-2024-12345.

Description: This section provides a concise summary of the vulnerability or exposure. It includes details such as the nature of the vulnerability (e.g., buffer overflow, SQL injection), the impact it may have (e.g., remote code execution, information disclosure), and the affected software or hardware. The description aims to give a clear understanding of what the issue is and why it is significant.

References: This element includes links and citations to additional resources related to the vulnerability. This may include advisories from vendors, patches, or other relevant documents. References help users and security professionals find more detailed information and guidance on how to address the vulnerability.

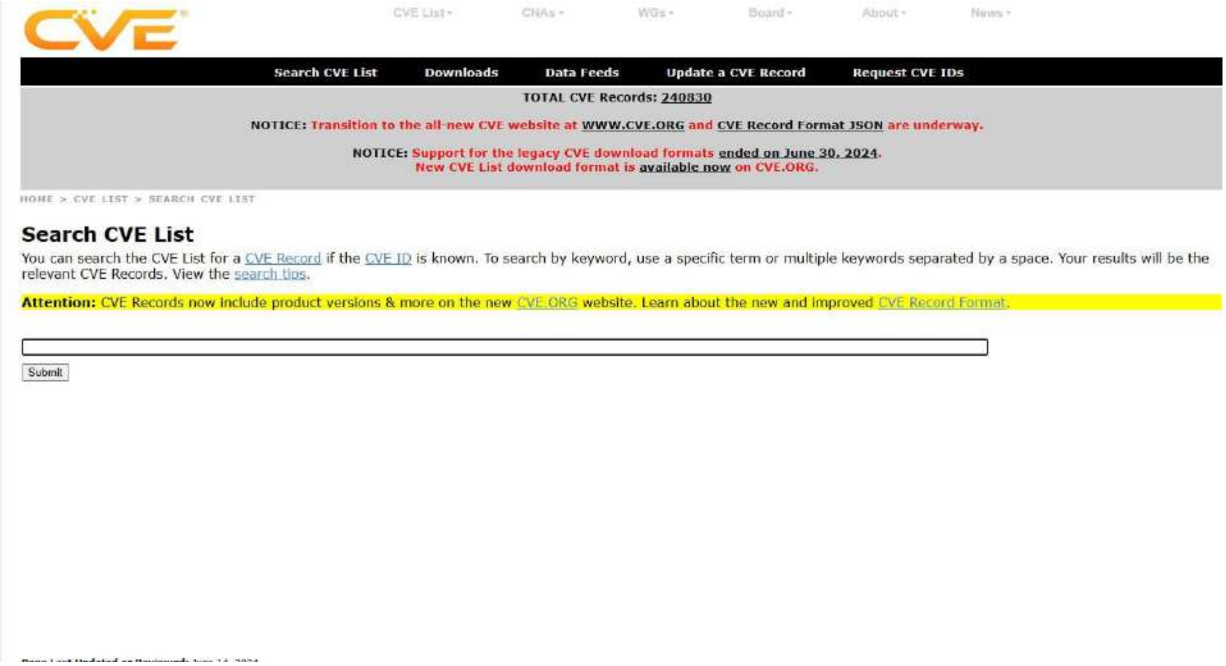
8. Scroll down to CVE List Basics. What is the process by which a vulnerability becomes a CVE listing? Who is involved in this process?

There is identification, reporting, review and assignment. This is then followed by drafting a description, compiling references, and then updating the database. The parties involved are CNA's, vulnerability reporters, Mitre, and affected vendors.

9. Click the link CVE Data Feeds. Scroll through the newest CVE entries feed. Were you aware of these vulnerabilities? How does the CVE distribute its information? Would you consider it sufficient? How can this be used by security personnel?

I was not aware of these vulnerabilities. The CVE distributes its information mainly by year from what is seen. I would consider it a decent way of distributing information, but not completely optimal. This can be used by security personel to see how vulnerabilities have evolved over time and from company to company so that they can prepare for what to expect

10. Click Search CVE List.



TOTAL CVE Records: 240830

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.

NOTICE: Support for the legacy CVE download formats ended on June 30, 2024.
New CVE List download format is available now on CVE.ORG.

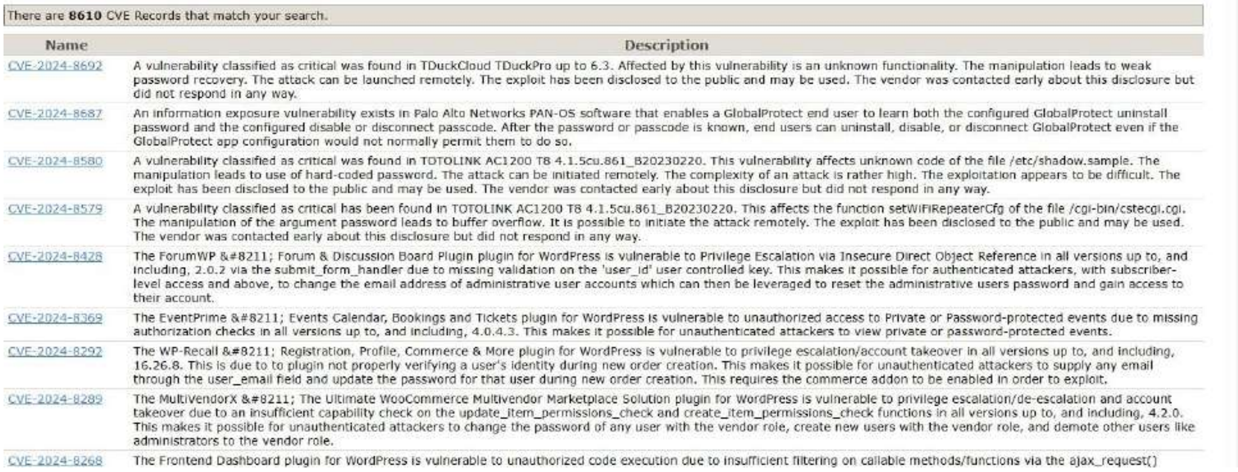
Search CVE List

You can search the CVE List for a CVE Record if the CVE ID is known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Records. View the search tips.

Attention: CVE Records now include product versions & more on the new CVE.ORG website. Learn about the new and improved CVE Record Format.

11. Enter a generic vulnerability such as passwords to display the CVE entries. How many are there that relate to this topic?

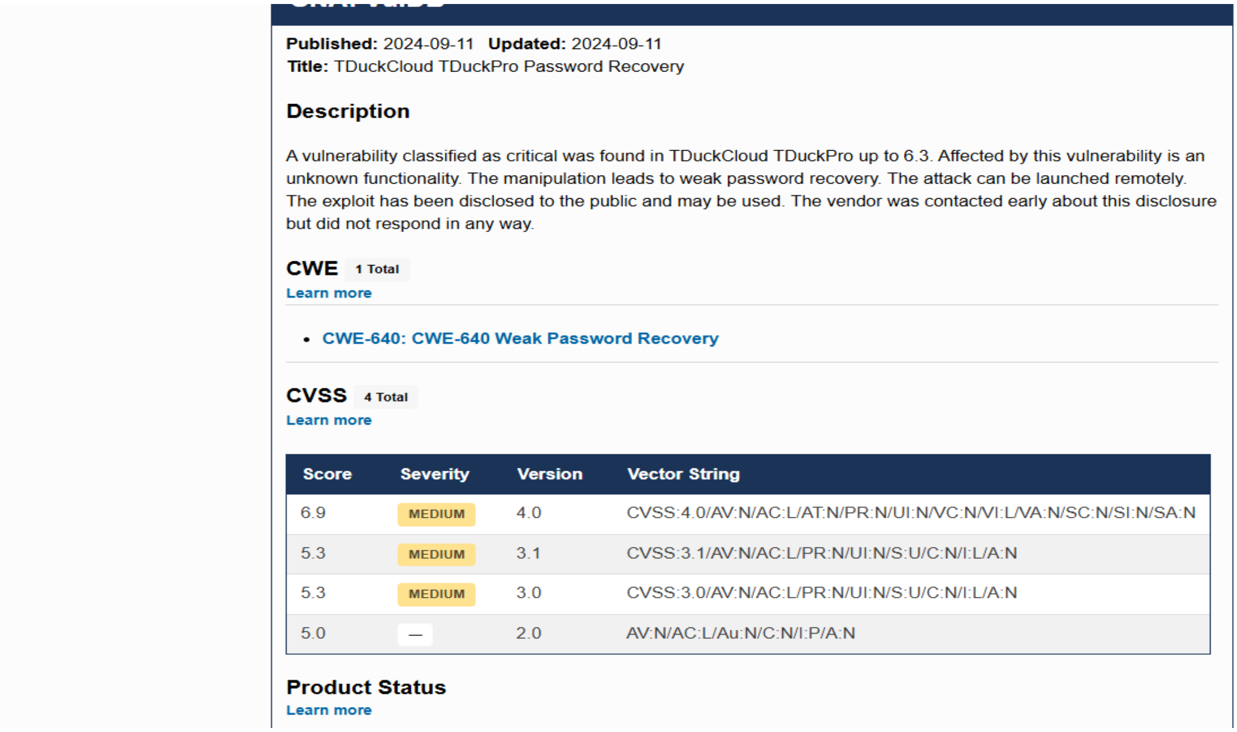
8610 results



There are **8610** CVE Records that match your search.

Name	Description
CVE-2024-8692	A vulnerability classified as critical was found in TDuckCloud TDuckPro up to 6.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to weak password recovery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-8687	An information exposure vulnerability exists in Palo Alto Networks PAN-OS software that enables a GlobalProtect end user to learn both the configured GlobalProtect uninstall password and the configured disable or disconnect passcode. After the password or passcode is known, end users can uninstall, disable, or disconnect GlobalProtect even if the GlobalProtect app configuration would not normally permit them to do so.
CVE-2024-8580	A vulnerability classified as critical was found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This vulnerability affects unknown code of the file /etc/shadow.sample. The manipulation leads to use of hard-coded password. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-8579	A vulnerability classified as critical has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220. This affects the function setWiFiRepeaterCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument password leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-8428	The ForumWP &#8211; Forum & Discussion Board Plugin plugin for WordPress is vulnerable to Privilege Escalation via Insecure Direct Object Reference in all versions up to, and including, 2.0.2 via the submit_form_handler due to missing validation on the 'user_id' user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to change the email address of administrative user accounts which can then be leveraged to reset the administrative users password and gain access to their account.
CVE-2024-8369	The EventPrime &#8211; Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized access to Private or Password-protected events due to missing authorization checks in all versions up to, and including, 4.0.4.3. This makes it possible for unauthenticated attackers to view private or password-protected events.
CVE-2024-8292	The WP-Recall &#8211; Registration, Profile, Commerce & More plugin for WordPress is vulnerable to privilege escalation/account takeover in all versions up to, and including, 16.26.8. This is due to to plugin not properly verifying a user's identity during new order creation. This makes it possible for unauthenticated attackers to supply any email through the user_email field and update the password for that user during new order creation. This requires the commerce addon to be enabled in order to exploit.
CVE-2024-8289	The MultiVendorX &#8211; The Ultimate WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to privilege escalation/de-escalation and account takeover due to an insufficient capability check on the update_item_permissions_check and create_item_permissions_check functions in all versions up to, and including, 4.2.0. This makes it possible for unauthenticated attackers to change the password of any user with the vendor role, create new users with the vendor role, and demote other users like administrators to the vendor role.
CVE-2024-8268	The Frontend Dashboard plugin for WordPress is vulnerable to unauthorized code execution due to insufficient filtering on callable methods/functions via the ajax_request()

12. Select several of the CVE entries and read through the material.



Published: 2024-09-11 **Updated:** 2024-09-11
Title: TDuckCloud TDuckPro Password Recovery

Description

A vulnerability classified as critical was found in TDuckCloud TDuckPro up to 6.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to weak password recovery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

CWE 1 Total
Learn more

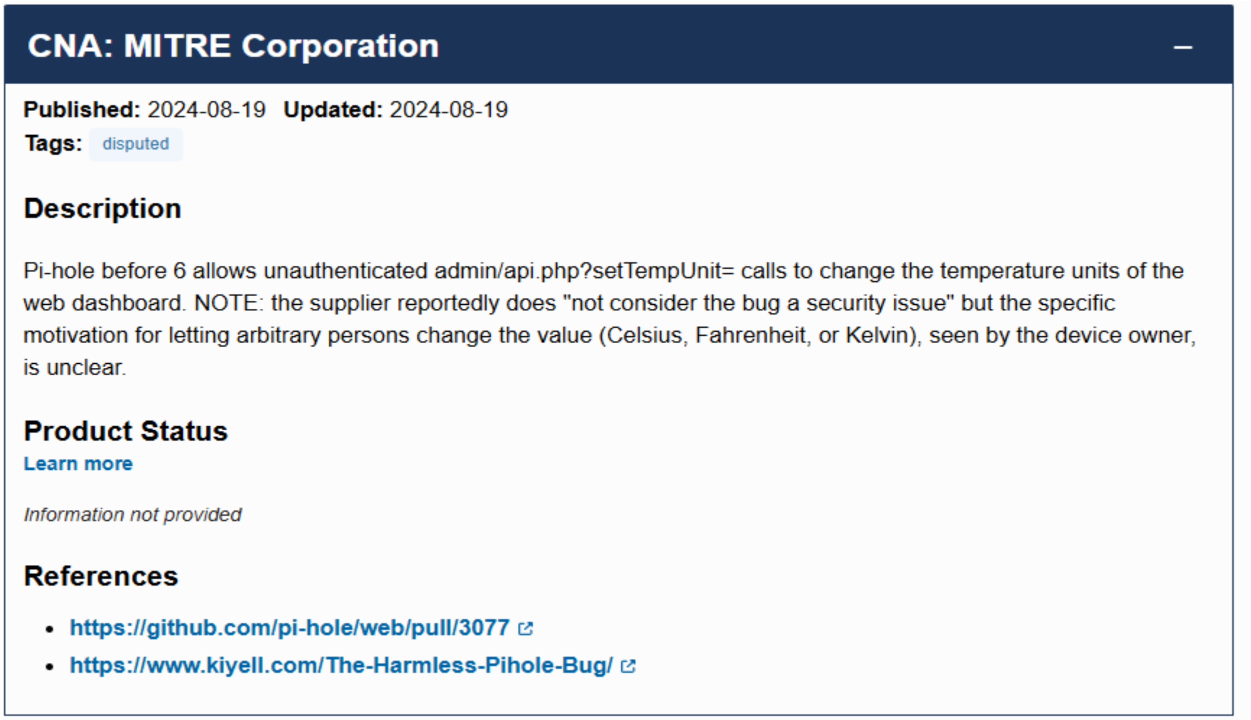
- CWE-640: CWE-640 Weak Password Recovery

CVSS 4 Total
Learn more

Score	Severity	Version	Vector String
6.9	MEDIUM	4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
5.3	MEDIUM	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
5.3	MEDIUM	3.0	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
5.0	—	2.0	AV:N/AC:L/Au:N/C:N/I:P/A:N

Product Status
Learn more

13. Locate a CVE entry that contains the tag Disputed. Click this entry. Under Description click **DISPUTED** to read about what constitutes a disputed CVE. Who would dispute a CVE? Why?



CNA: MITRE Corporation

Published: 2024-08-19 **Updated:** 2024-08-19
Tags: disputed

Description

Pi-hole before 6 allows unauthenticated admin/api.php?setTempUnit= calls to change the temperature units of the web dashboard. NOTE: the supplier reportedly does "not consider the bug a security issue" but the specific motivation for letting arbitrary persons change the value (Celsius, Fahrenheit, or Kelvin), seen by the device owner, is unclear.

Product Status

Learn more

Information not provided

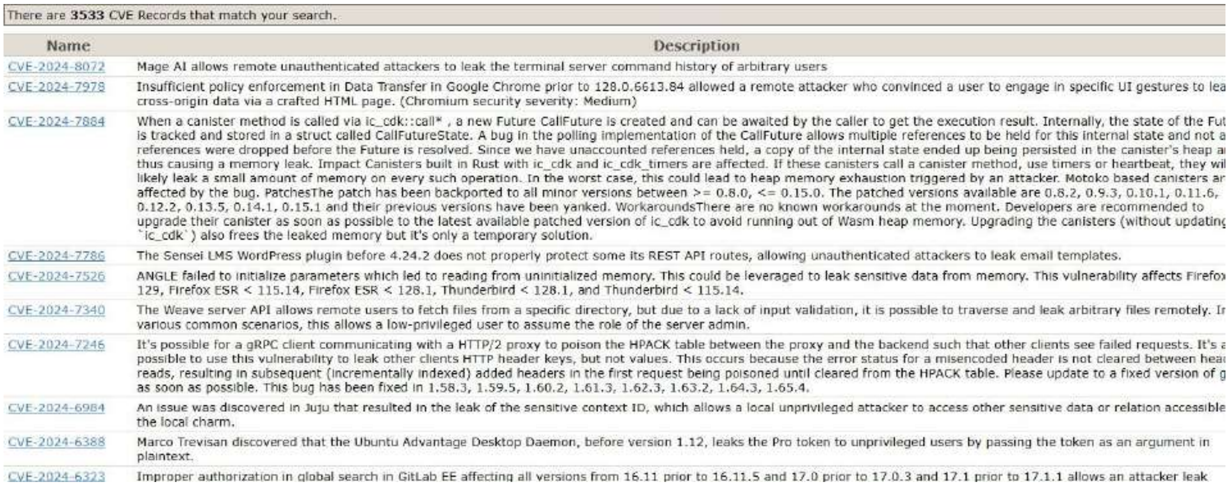
References

- https://github.com/pi-hole/web/pull/3077
- https://www.kiyell.com/The-Harmless-Pihole-Bug/

There are many things that can constitute a dispute, but some are accuracy of information, or duplicate entries. This can be done by vendors, researchers, the CNA, or security teams. This is all essential for the accuracy of information

14. Click Search CVE List.

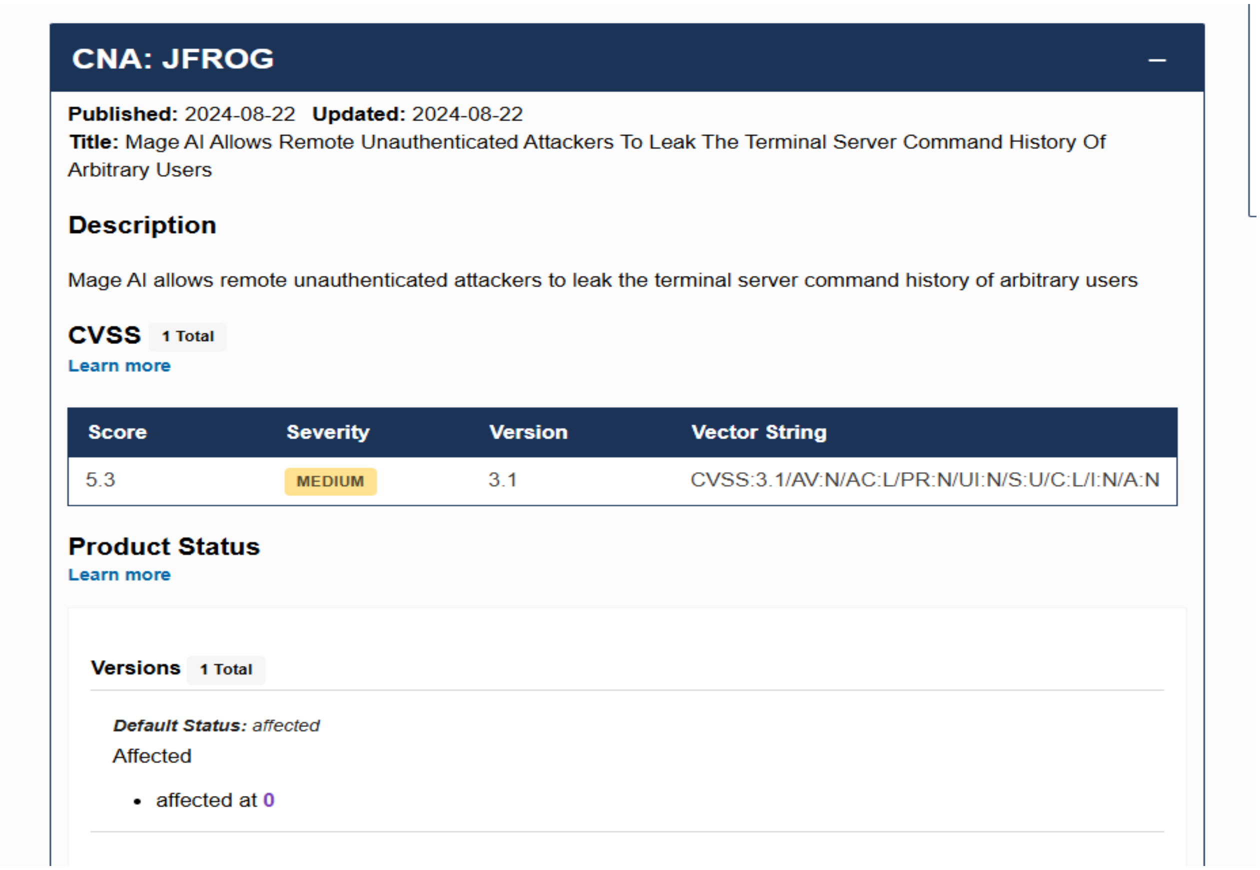
“leak”



There are **3533** CVE Records that match your search.

Name	Description
CVE-2024-8072	Mage AI allows remote unauthenticated attackers to leak the terminal server command history of arbitrary users
CVE-2024-7978	Insufficient policy enforcement in Data Transfer in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who convinced a user to engage in specific UI gestures to lea cross-origin data via a crafted HTML page. (Chromium security severity: Medium)
CVE-2024-7884	When a canister method is called via ic_cdk::call* , a new Future CallFuture is created and can be awaited by the caller to get the execution result. Internally, the state of the Fut is tracked and stored in a struct called CallFutureState. A bug in the polling implementation of the CallFuture allows multiple references to be held for this internal state and not a references were dropped before the Future is resolved. Since we have unaccounted references held, a copy of the internal state ended up being persisted in the canister's heap ar thus causing a memory leak. Impact Canisters built in Rust with ic_cdk and ic_cdk_timers are affected. If these canisters call a canister method, use timers or heartbeat, they wil likely leak a small amount of memory on every such operation. In the worst case, this could lead to heap memory exhaustion triggered by an attacker. Motoko based canisters ar affected by the bug. PatchesThe patch has been backported to all minor versions between >= 0.8.0, <= 0.15.0. The patched versions available are 0.8.2, 0.9.3, 0.10.1, 0.11.6, 0.12.2, 0.13.5, 0.14.1, 0.15.1 and their previous versions have been yanked. WorkaroundsThere are no known workarounds at the moment. Developers are recommended to upgrade their canister as soon as possible to the latest available patched version of ic_cdk to avoid running out of Wasm heap memory. Upgrading the canisters (without updating \`ic_cdk\`) also frees the leaked memory but it's only a temporary solution.
CVE-2024-7786	The Sensei LMS WordPress plugin before 4.24.2 does not properly protect some its REST API routes, allowing unauthenticated attackers to leak email templates.
CVE-2024-7526	ANGLE failed to initialize parameters which led to reading from uninitialized memory. This could be leveraged to leak sensitive data from memory. This vulnerability affects Firefox 129, Firefox ESR < 115.14, Firefox ESR < 128.1, Thunderbird < 128.1, and Thunderbird < 115.14.
CVE-2024-7340	The Weave server API allows remote users to fetch files from a specific directory, but due to a lack of input validation, it is possible to traverse and leak arbitrary files remotely. Ir various common scenarios, this allows a low-privileged user to assume the role of the server admin.
CVE-2024-7246	It's possible for a gRPC client communicating with a HTTP/2 proxy to poison the HPACK table between the proxy and the backend such that other clients see failed requests. It's a possible to use this vulnerability to leak other clients HTTP header keys, but not values. This occurs because the error status for a misencoded header is not cleared between hea reads, resulting in subsequent (incrementally indexed) added headers in the first request being poisoned until cleared from the HPACK table. Please update to a fixed version of g as soon as possible. This bug has been fixed in 1.58.3, 1.59.5, 1.60.2, 1.61.3, 1.62.3, 1.63.2, 1.64.3, 1.65.4.
CVE-2024-6984	An issue was discovered in Juju that resulted in the leak of the sensitive context ID, which allows a local unprivileged attacker to access other sensitive data or relation accessible the local charm.
CVE-2024-6388	Marco Trevisan discovered that the Ubuntu Advantage Desktop Daemon, before version 1.12, leaks the Pro token to unprivileged users by passing the token as an argument in plaintext.
CVE-2024-6323	Improper authorization in global search in GitLab EE affecting all versions from 16.11 prior to 16.11.5 and 17.0 prior to 17.0.3 and 17.1 prior to 17.1.1 allows an attacker leak

15. Enter a different vulnerability and select several entries to read through its details.



CNA: JFROG

Published: 2024-08-22 **Updated:** 2024-08-22
Title: Mage AI Allows Remote Unauthenticated Attackers To Leak The Terminal Server Command History Of Arbitrary Users

Description

Mage AI allows remote unauthenticated attackers to leak the terminal server command history of arbitrary users

CVSS 1 Total
Learn more

Score	Severity	Version	Vector String
5.3	MEDIUM	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Product Status
Learn more

Versions 1 Total

Default Status: *affected*
Affected

- affected at 0

16. Close all windows

References:

Mitre. (1999). *CVE website*. CVE Website. https://www.cve.org/

Case project 2-1: False Positives and False Negatives

Use the Internet to research false positives and false negatives. Which is worse? If a doctor gives information to a patient about the results of a diagnostic test, is a false positive or a false negative worse? What about facial recognition scanning for a criminal? Which is worse for a vulnerability scan, a false positive or a false negative? Write a one-page paper on your findings and analysis

Introduction:

in cybersecurity, understanding the implications of false positives and false negatives is crucial for maintaining the effectiveness of security measures and ensuring the integrity of systems. Both types of errors can have significant impacts, but their severity and implications vary depending on the context.

A false positive in cybersecurity occurs when a security tool or vulnerability scanner incorrectly identifies a non-existent threat or vulnerability. For instance, a vulnerability scanner might flag a benign software component as a security risk. This can lead to several issues such as rescource drain, operational disruptions, or alert fatigue. Resource drain is when time and resources are spent investigating and mitigating non-existent threats, which can divert attention from real security concerns. Operational Disruptions: False positives can lead to unnecessary changes or patches being applied, potentially disrupting normal operations or causing system instability. And an example of alert fatigue would be Frequent false positives that can desensitize security teams to alerts, potentially leading them to overlook genuine threats.

On the other hand, a false negative occurs when a security tool fails to detect an actual threat or vulnerability. This error can have more severe consequences like security breaches, increased risk factors, and delayed responses. For security breaches, a missed vulnerability can be exploited by attackers, leading to data breaches, financial loss, or damage to the organization's reputation. Meanwhile the failure to identify real threats means that attackers have a higher chance of successfully compromising systems without detection would be the increased risk. For delayed responses, the longer a real threat goes undetected, the more damage it can cause, and the harder it can be to mitigate once discovered.

When evaluating which type of error is worse, in my opinion its false negatives because they generally pose a greater risk. This is because the primary goal of security measures is to detect and mitigate genuine threats to protect systems and data. A false negative can leave systems exposed to actual attacks, potentially leading to severe consequences including data breaches, financial loss, and reputational damage.

Although false positives can be disruptive and lead to inefficiencies, they do not pose the same level of risk as false negatives. False positives typically result in operational inefficiencies and increased workload, but they do not inherently expose the system to real threats. The critical nature of identifying and responding to actual vulnerabilities makes false negatives more dangerous and impactful.

Regarding false positives and negatives, false negatives are more detrimental compared to false positives. The primary concern is to ensure that all real threats are identified and addressed to prevent security breaches and protect sensitive information. While false positives can lead to inefficiencies and operational disruptions, the risk of not detecting a genuine threat is significantly higher and more damaging. Therefore, cybersecurity professionals must focus on reducing false negatives to enhance the overall security of their systems.

References:

Santos, M. (2021, September 22). *False positives vs. false negatives*. Medium. https://towardsdatascience.com/false-positives-vs-false-negatives-4184c2ff941a

Case Project 2-3: Vulnerability Scanners

Search the Internet for information on Nessus. Then search for two other vulnerability scanners. Create a table that compares their features. Which would you choose? Why

Introduction

Nessus is a vulnerability scanner by Tenable which helps expose and close weaknesses across a computer and gives a highly detailed report (Tenable, n.d.). Besides Nessus, there are other vulnerability scanner which will be discussed in this case project, which are mainly used to assess a business' cybersecurity in several aspects. The scanners can be used to check networks, systems, applications, security vulnerabilities, and more.

NESSUS	Invicti	Stackhawk
Web application scans, external attack surface scans, cloud infrastructure scans	Scan websites, applications, API, cloud	Run as many scans across all applications and environments, and with unlimited access for users.
Unlimited IT vulnerability assessments	Ai Risk prediction	Designed for development environments for people coding
Vulnerability scoring with CVSS v4, EPSS and VPR	Finds every high-risk vulnerability, great accuracy	Track scan data and gain insight into vulnerabilities over time and across environments.
Configuration, compliance and security audits	Report with assistance in fixing and locating vulnerabilities	Automation and notifications to speed up fixes
Configurable reports	Security automation with configurable automatic fixes and scans	Scan validation and authentication to scan all applications
On-demand training and advanced support	Tracking analytics, notifications, and configuration	API support & regular custom support
Free 7-day trial, but several thousand to	Demo, need a quote to purchase (probably in the	14 day free trial, $42-$59 per code contributor

purchase	thousands)	

References

Invicti. (n.d.). *How Invicti paves your road to security*. Retrieved from invicti: https://www.invicti.com/features/

Microsoft. (n.d.). *What is a virtual machine (VM)?* Retrieved from Microsoft: https://azure.microsoft.com/en-us/resources/cloud-computing- dictionary/what-is-a-virtual-machine

Scale Computing. (2023, September 25). *Understanding Virtual Machine Advantages and Disadvantages*. Retrieved from Scale Computing: https://www.scalecomputing.com/resources/understanding-virtual-machine-advantages-and-disadvantages

Stackhawk. (n.d.). *Application Security at the*. Retrieved from Stackhawk: https://www.stackhawk.com/pricing/

Tenable. (n.d.). *Nessus Vulnerability Scanner: Network Security Solution*. Retrieved from Tenable: https://www.tenable.com/products/nessus

Assignment 2 - Hands On

Sam Peller

September 12, 2024

ISM 4323

Project 3-1: analyze File and Url for File-Based Viruses Using VirusTotal—part 1

Time required: 25 minutes

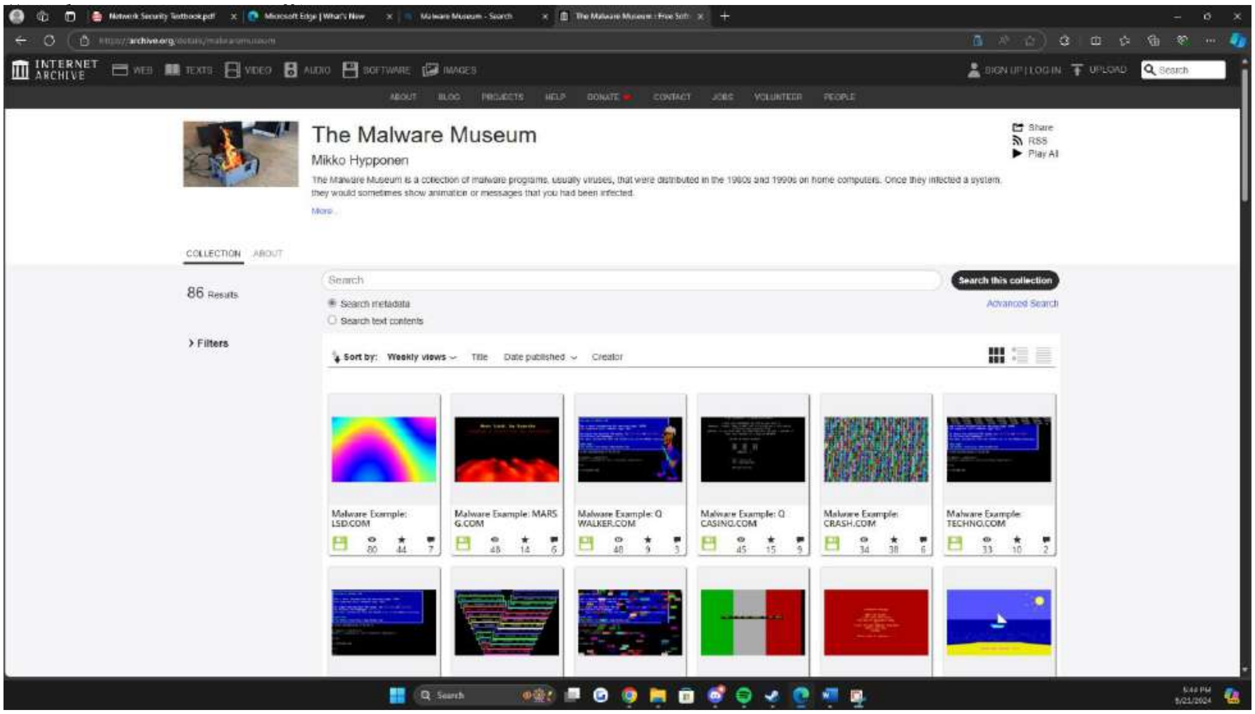
objective: Given a scenario, analyze potential indicators to determine the type of attack.

description: VirusTotal is a free online service that analyzes files and urls to identify potential malware. VirusTotal combines 70 antivirus scanners and url/domain blacklisting services along with other tools to identify malware. A wide range of files can be submitted to VirusTotal for examination, such as user data files and documents, executable programs, pdFs, and images. one of the uses of VirusTotal is to provide a “second opinion” on a file or url that may have been flagged as suspicious by other scanning software. In this project, you use VirusTotal to scan a file and a url.

INTRODUCTION

When clicking a link sent by someone you don’t trust or downloading a file, it’s always good to do a quick double check to make sure nothing bad is going on. VirusTotal was made for things like this, as it states it, “Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches,” (VirusTotal, n.d.) Files and URLs are two major sources of cyber-attacks when it comes to executables and cross-site scripting. A free tool to keep you safe online.

1. **First view several viruses from 20 years ago and observe their benign but annoying impact. open your web browser and enter the url archive.org/details/malwaremuseumstab=collection (if you are no longer able to access the site through the web address, use a search engine to search for**

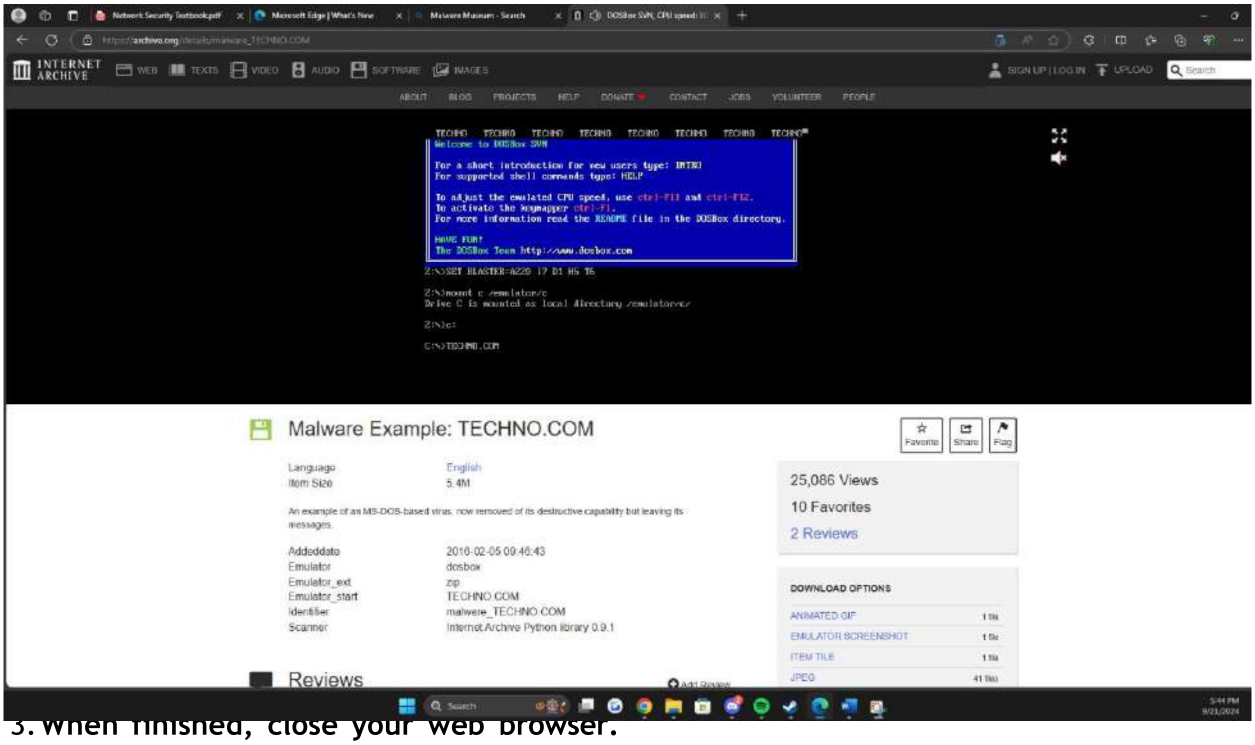


The Malware Museum

Mikko Hypponen

The Malware Museum is a collection of malware programs, usually viruses, that were distributed in the 1980s and 1990s on home computers. Once they infected a system, they would sometimes show animation or messages that you had been infected.

2. All of the viruses have been rendered ineffective and will not harm a computer. click several of the viruses and notice what they do.



```
TECHNO  TECHNO  TECHNO  TECHNO  TECHNO  TECHNO  TECHNO  TECHNO
Welcome to DOSBox SVN

For a short introduction for new users type: INTRO
For supported shell commands type: HELP

To adjust the emulated CPU speed, use ctrl-F11 and ctrl-F12.
To activate the keymapper ctrl-F1.
For more information read the README file in the DOSBox directory.

HAVE FUN!
The DOSBox Team http://www.dosbox.com
Z:\>SET BLASTER=A220 I7 D1 H5 T6

Z:\>mount c /emulator/c
Drive C is mounted as local directory /emulator/c/

Z:\>c:

C:\>TECHNO.COM
```

Malware Example: TECHNO.COM

Language	English
Item Size	5.4M

An example of an MS-DOS-based virus, now removed of its destructive capability but leaving its messages.

Addeddate	2016-02-05 09:46:43
Emulator	dosbox
Emulator_ext	zip
Emulator_start	TECHNO.COM
Identifier	malware_TECHNO.COM
Scanner	Internet Archive Python library 0.9.1

25,086 Views

10 Favorites

2 Reviews

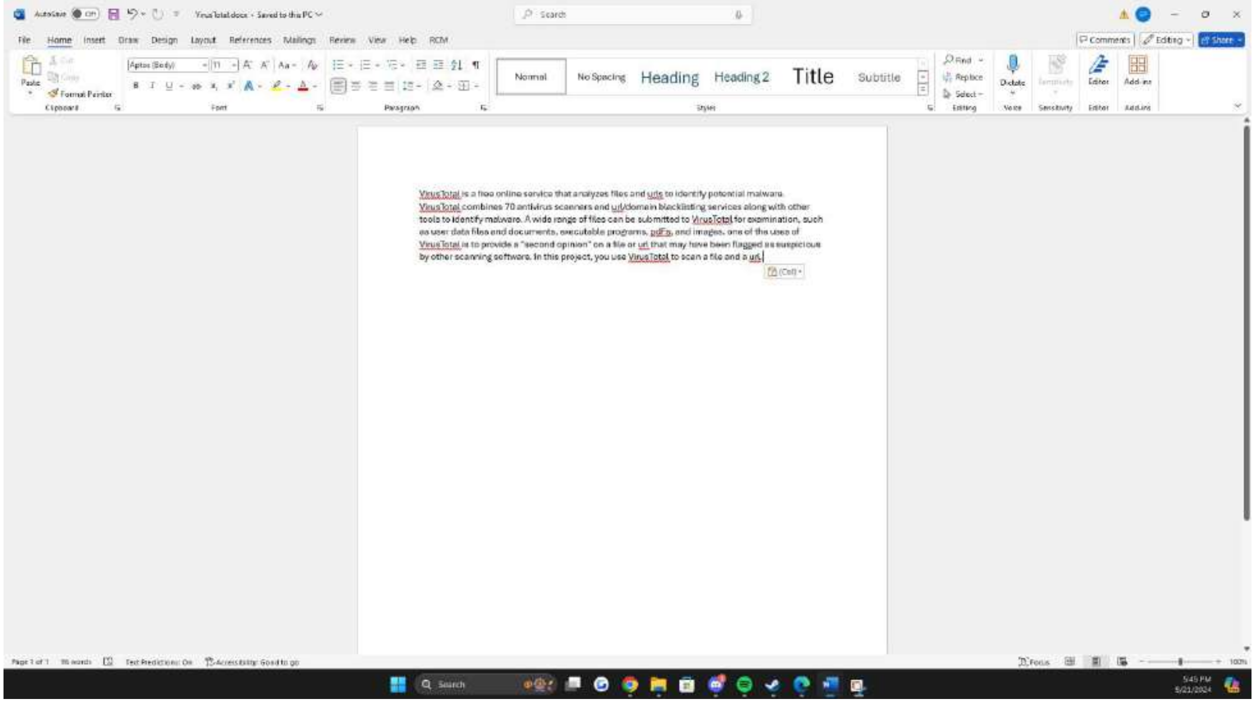
DOWNLOAD OPTIONS

ANIMATED GIF	1 file
EMULATOR SCREENSHOT	1 file
ITEM TILE	1 file
JPEG	41 files

Reviews

3. When finished, close your web browser.

4. use Microsoft Word to create a document that contains the preceding paragraph description about VirusTotal. save the document as



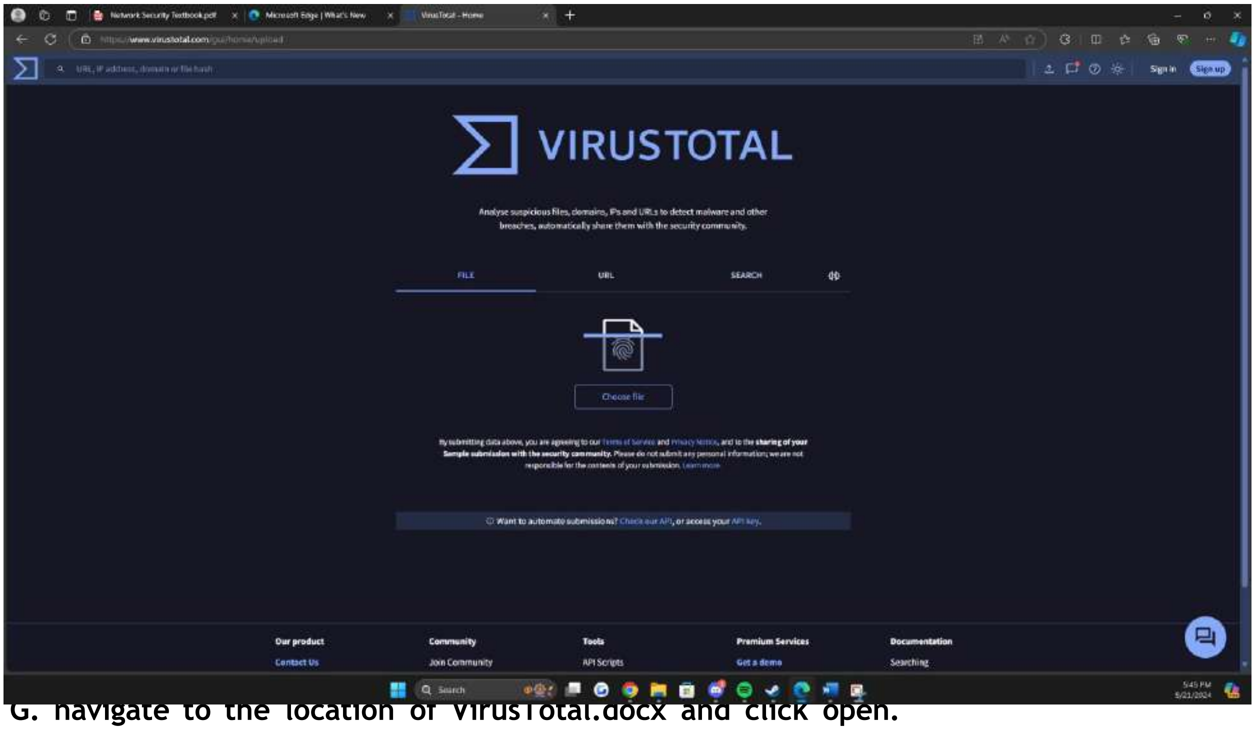
VirusTotal is a free online service that analyzes files and urls to identify potential malware. VirusTotal combines 70 antivirus scanners and url/domain blacklisting services along with other tools to identify malware. A wide range of files can be submitted to VirusTotal for examination, such as user data files and documents, executable programs, pdFs, and images. one of the uses of VirusTotal is to provide a "second opinion" on a file or url that may have been flagged as suspicious by other scanning software. In this project, you use VirusTotal to scan a file and a url.

5. exit Word.

6. open your web browser and enter the url www.virustotal.com (if you are no longer able to access the site through the web address, use a search engine to search for “Virus Total”).

7. If necessary, click the File tab.

8. click Choose File.



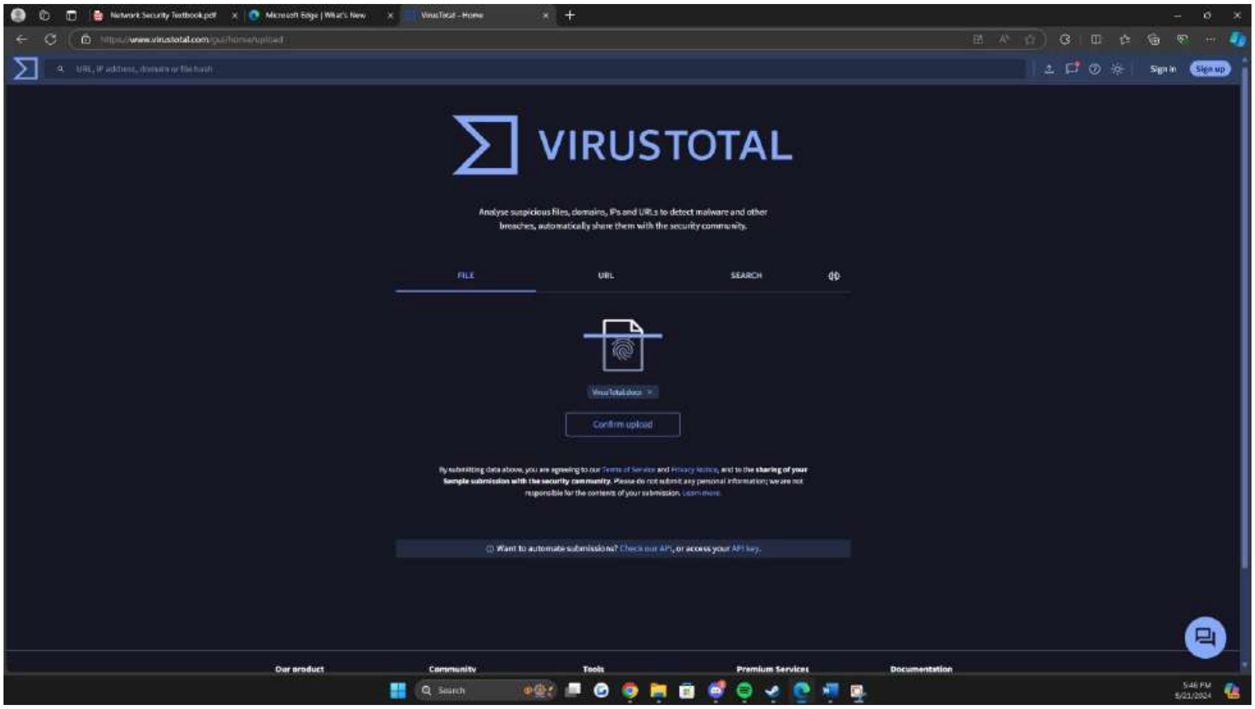
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, or access your API key.

9. navigate to the location of VirusTotal.docx and click open.

10. click Confirm upload.



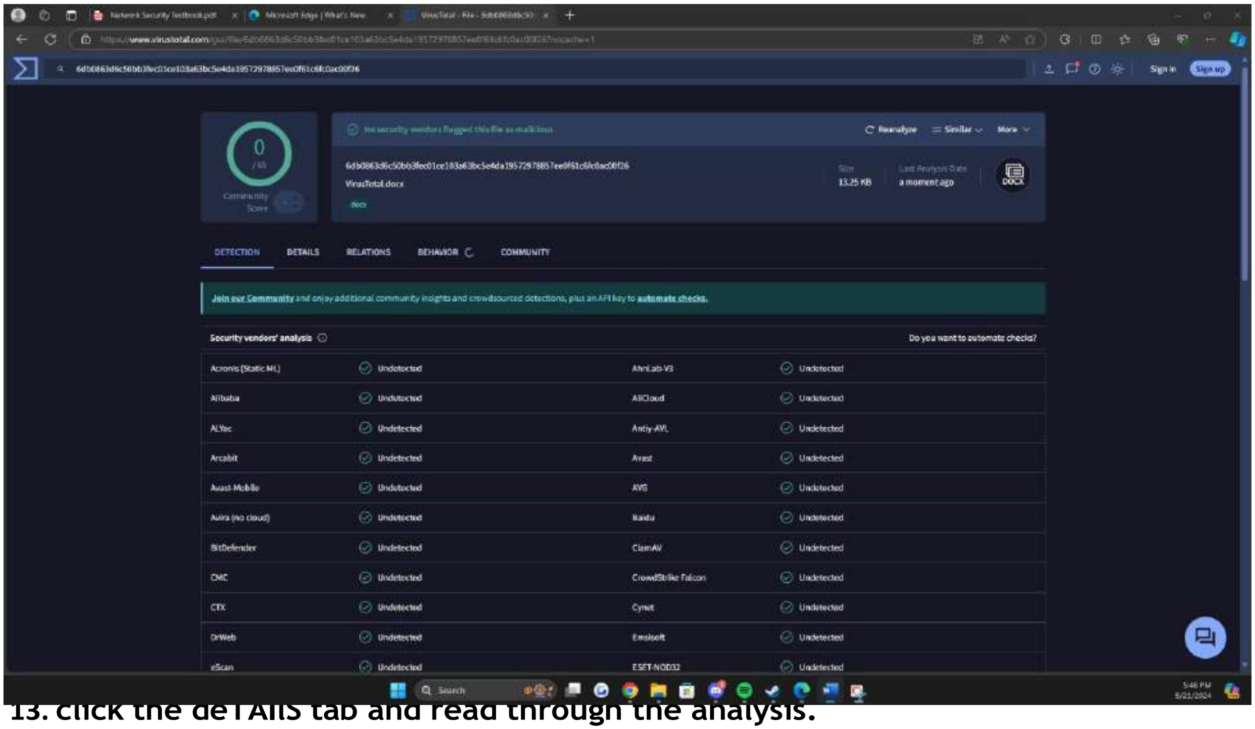
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, or access your API key.

11. Wait until the upload and analysis are completed.

12. scroll through the list of antivirus (AV) vendors that have been polled regarding this file. A green checkmark means no malware was detected.



No security vendors flagged this file as malicious

6db0863d6c50bb3fec01ce103a63bc5e4da19572978857ee0f61c6fc0ac00f26
VirusTotal.docx
docx

Size 13.25 KB
Last Analysis Date a moment ago

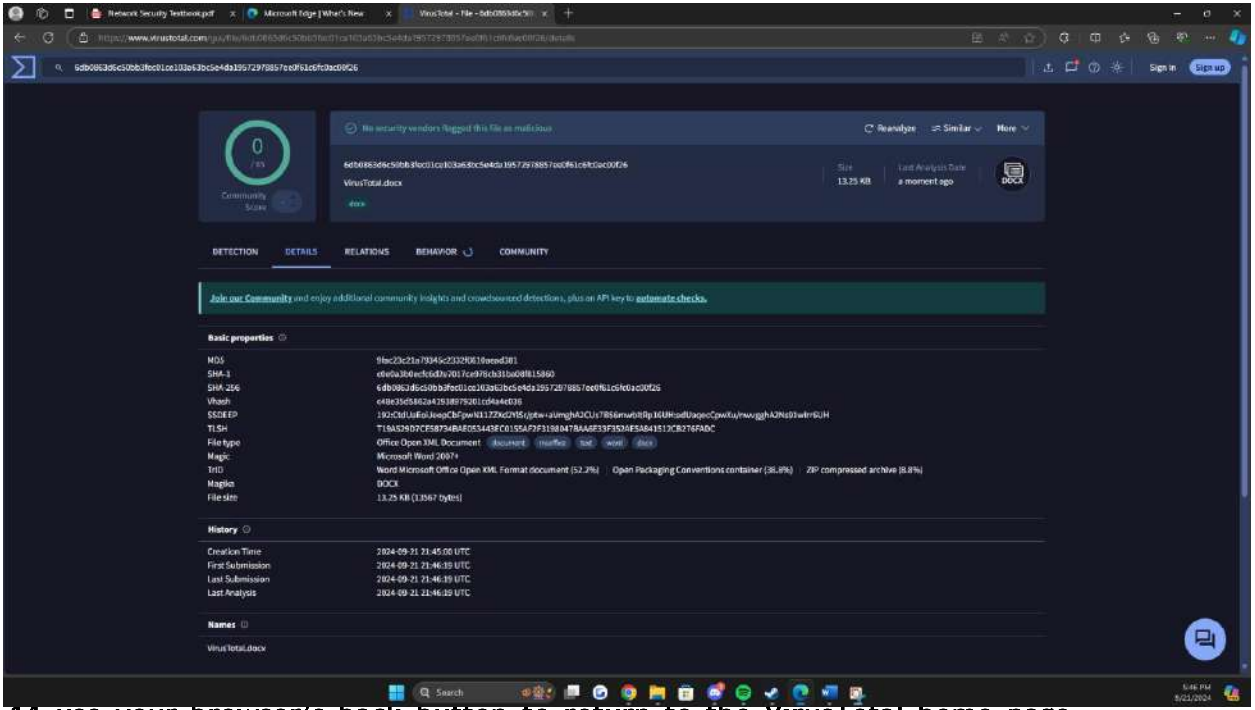
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected	AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avast-Mobile	✓ Undetected	AVG	✓ Undetected
Avira (no cloud)	✓ Undetected	Baidu	✓ Undetected
BitDefender	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	CrowdStrike Falcon	✓ Undetected
CTX	✓ Undetected	Cynet	✓ Undetected
DrWeb	✓ Undetected	Emsisoft	✓ Undetected
eScan	✓ Undetected	ESET-NOD32	✓ Undetected

13. click the deTAIlS tab and read through the analysis.



No security vendors flagged this file as malicious

6db0863d6c50bb3fec01ce103a63bc5e4da19572978857ee0f61c6fc0ac00f26
VirusTotal.docx
docx

Size 13.25 KB
Last Analysis Date a moment ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	9fac23c21a79345c2332f0610aead381
SHA-1	c0e0a3b0ecfc6d7e7017ce978cb31ba08f815860
SHA-256	6db0863d6c50bb3fec01ce103a63bc5e4da19572978857ee0f61c6fc0ac00f26
Vhash	e48e35d5862a42938979201cd4a4e036
SSDEEP	192:CtdUaEoiJeepCbFpwN11ZZXd2YlSr/ptw+aUmghA2CUs7B56mwbltRp16UHsdUaqecCpwXu/nwvgghA2Ns91wlrr6UH
TLSH	T19A529D7CE58734BAE053443EC0155AF2F3198047BAA6E33F352AE5A841512CB276FADC
File type	Office Open XML Document document msoffice text word docx
Magic	Microsoft Word 2007+
TrID	Word Microsoft Office Open XML Format document (52.2%) Open Packaging Conventions container (38.8%) ZIP compressed archive (8.8%)
Magika	DOCX
File size	13.25 KB (13567 bytes)

History

Creation Time	2024-09-21 21:45:00 UTC
First Submission	2024-09-21 21:46:19 UTC
Last Submission	2024-09-21 21:46:19 UTC
Last Analysis	2024-09-21 21:46:19 UTC

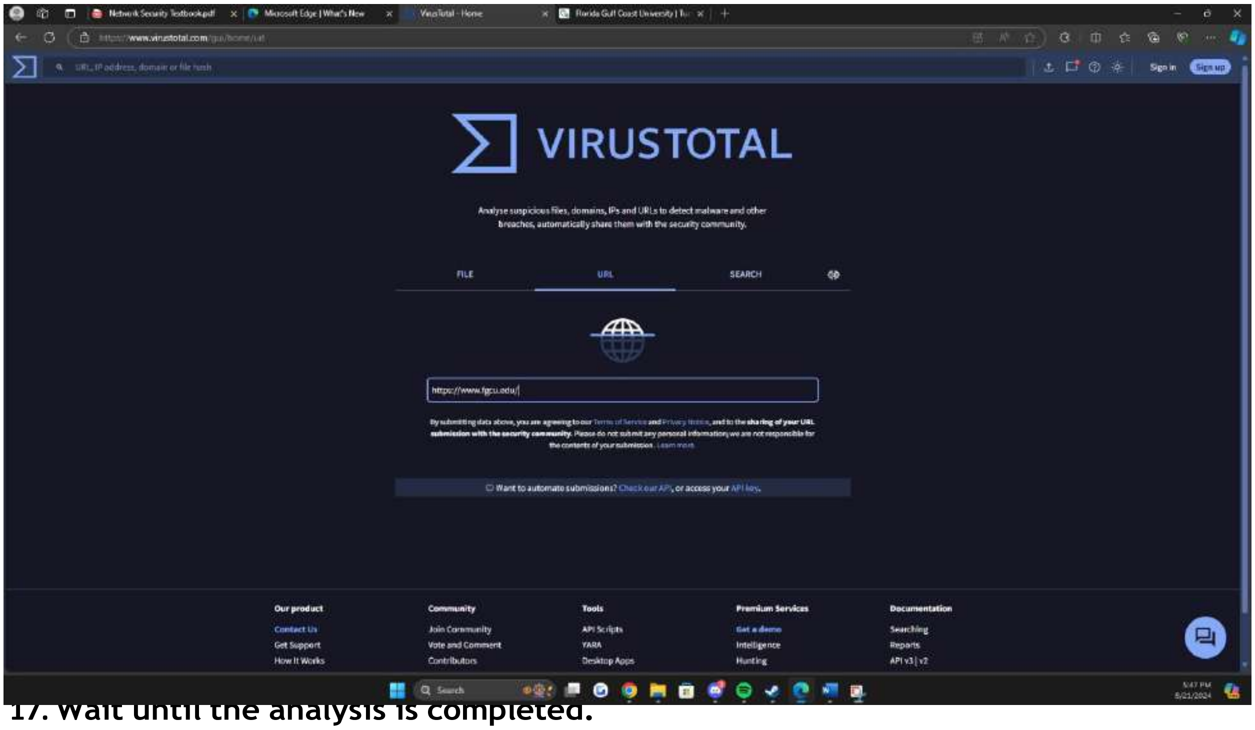
Names

VirusTotal.docx

14. use your browser’s back button to return to the VirusTotal home page.

15. now you will analyze a website. click url.

16. enter the url of your school, place of employment, or another site with which you are familiar.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

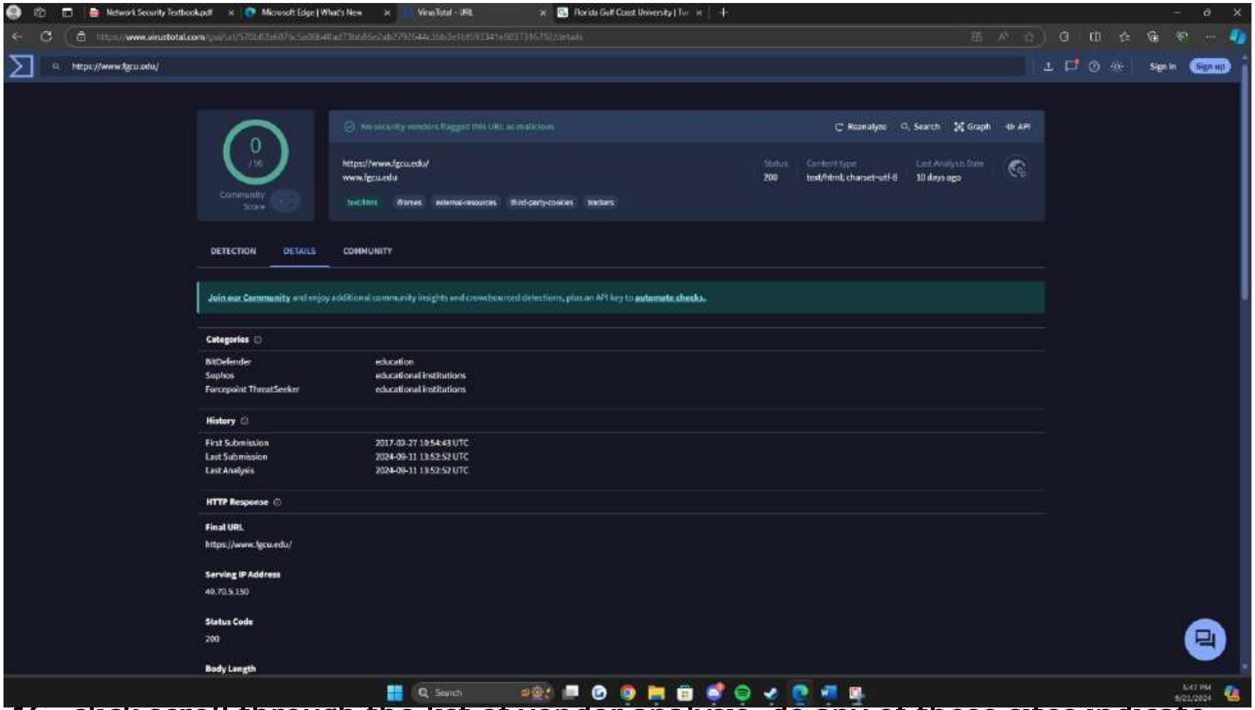
https://www.fgcu.edu/

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your URL submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, or access your API key.

17. wait until the analysis is completed.

18. click the deTAIlS tab and read through the analysis.



https://www.fgcu.edu/

0 / 96 Community Score

No security vendors flagged this URL as malicious

https://www.fgcu.edu/
www.fgcu.edu

Status	Content type	Last Analysis Date
200	text/html; charset=utf-8	10 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

BitDefender	education
Sophos	educational institutions
Forcepoint ThreatSeeker	educational institutions

History

First Submission	2017-02-27 10:54:43 UTC
Last Submission	2024-09-11 13:52:52 UTC
Last Analysis	2024-09-11 13:52:52 UTC

HTTP Response

Final URL
https://www.fgcu.edu/

Serving IP Address
40.70.5.150

Status Code
200

Body Length

19. click scroll through the list of vendor analysis. do any of these sites indicate unrated site or Malware site? Yes, at least 25.

20. how could VirusTotal be useful to users? how could it be useful to security researchers? could it also be used by attackers to test their own malware before distributing it to ensure that it does not trigger an AV alert? What should be the protections against this?

Most users when downloading something or visiting a site want to know if it is safe to do so, personally I've used virustotal in these situations to ensure my safety. Safety researchers can use it to analyze new malware or see how accurate threat intelligence is. It could be used my attackers to test their own malware, but I'm sure at least one of these constantly updating antivirus' would be able to detect it. It would also be advantageous for virustotal to rate limit submissions to ensure that this wouldn't happen.

21. close all windows

Case project 3-2: LOLBins

Prompt: Fileless viruses take advantage of native services and processes that are part of the OS to avoid detection and carry out their attacks. These native services used in a fileless virus are called living-off-the-land binaries (LOLBins). Use the Internet to research fileless viruses and LOLBins.
When did fileless viruses first appear? How do they compare with file-based viruses? What are the defenses against fileless viruses? Write a one-page paper on your research

Introduction:

Fileless viruses represent a growing threat in the cybersecurity landscape, they leverage native operating system services and processes to execute attacks without relying on traditional files. These malicious entities utilize living-off-the-land binaries (LOLBins), which are legitimate tools within the OS, making them difficult to detect and mitigate[1]. This paper will explore the history of fileless viruses, their differences from file-based viruses, and potential defenses against these sophisticated attacks.

Fileless malware has its roots in the early 2010s, but it gained significant attention around 2017 with high-profile attacks such as the PowerShell-based attacks used in the Equifax breach[2]. Unlike traditional malware that requires a malicious file to be downloaded or executed, fileless viruses execute directly in memory, leveraging built-in OS tools and scripts, particularly PowerShell and Windows Management Instrumentation. This evolution has led to an increase in the use of fileless techniques among cybercriminals, as they can bypass traditional detection methods that focus on file-based signatures.

File-based viruses essentially operate by infecting files on a system, which often relies on user interaction to spread. They can be detected through signature-based antivirus solutions, which scan for known malicious files. In contrast, fileless viruses are more elusive; they often reside only in memory and do not leave traditional footprints on disk. This means they can execute their payloads without triggering alerts from conventional security measures[3]. The use of LOLBins adds another layer of complexity, as these are trusted system tools that can be manipulated for malicious purposes, further obscuring the attacker's presence.

Defending against fileless attacks requires a multi-faceted approach. The first being Behavioral Analysis which would utilize Security solutions that analyze the behavior of processes to identify anomalies indicative of fileless malware, such as unusual PowerShell[4] commands or

[1] (K7, 2022)
[2] (Adebayo, 2023)
[3] (Staff, 2024)
[4] (Neagu, 2023)

WMI queries. Another beneficial solution would be EDR solutions to provide real-time monitoring and response capabilities, focusing on the behavior of running processes rather than just file- based indicators[5]. Also, Application Whitelisting allows only approved applications and scripts to run, organizations can significantly reduce the attack surface available to fileless malware.
Meanwhile you could use PowerShell Constrained Language Mode which restricts the functionality of PowerShell, limiting what scripts can do and thereby reducing the potential for abuse. Finally, user education and awareness can train users to recognize phishing attempts, and suspicious activity can help prevent the initial compromise that often leads to fileless attacks.

Fileless viruses pose a significant challenge to cybersecurity due to their ability to evade traditional detection mechanisms by utilizing native OS services and tools. As they become more prevalent, it is crucial for organizations to adopt advanced detection methods and robust security practices. By focusing on behavior-based analysis, endpoint protection, and user education, organizations can strengthen their defenses against this evolving threat. The landscape of malware continues to shift, and staying informed about these trends is essential for effective cybersecurity strategies.

[5] (Floreza, 2018)

References:

Adebayo, K. S. (2023, December 8). *Equifax's lessons are still relevant, 5 years later*. Equifax's Lessons Are Still Relevant, 5 Years Later. https://www.darkreading.com/cyberattacks-data- breaches/5-years-after-the-equifax-breach-industry-experts-share-new-insights

Fileless malware and LOLBins: Everything you should know. k7 Security. (2022, September 20). https://blog.k7computing.com/fileless-malware-and-lolbins-everything-you-should- know/#:~:text=Significant%20cyber-attacks%20exploiting%20LOLBins-%20A%20Timeline.

Floreza, S. (2018). *Security 101: Defending against fileless malware*. Trend Micro (US). https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101- defending-against-fileless-malware#:~:text=Fileless%20malware%20are%20a%20growing%20threat

Neagu, C. (2023, August 15). *What is PowerShell and how do you use it?*. Digital Citizen. https://www.digitalcitizen.life/simple-questions-what-powershell-what-can-you-do-it/#:~:text=PowerShell%20is%20a%20powerful%20scripting%20language

Staff, E. (2024, August 19). *File-infecting virus*. DevX. https://www.devx.com/terms/file-infecting- virus/#:~:text=A%20file-infecting%20virus%20is%20a%20type%20of%20malicious,causing%20damage%2C%20data%20corruption%2C%20or%20other%20unwanted%20effects.

project 5-1: creating and using Qr codes

Time required: 15 minutes

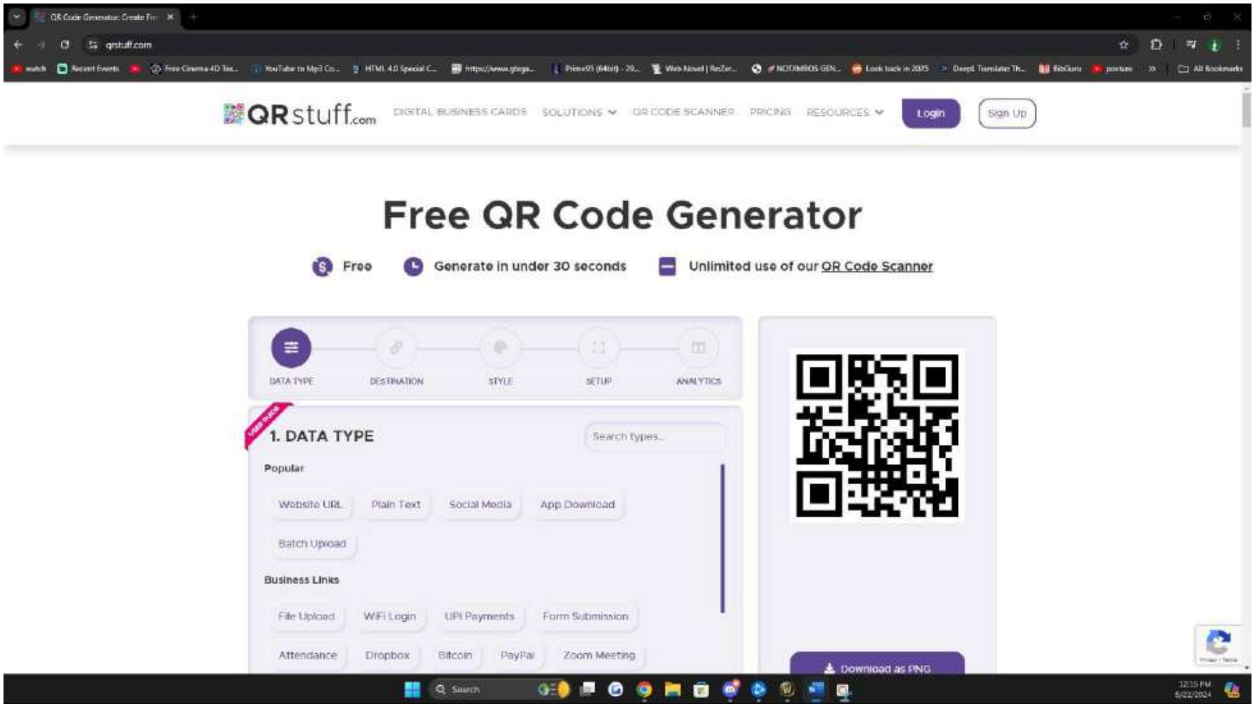
Objective: Given a scenario, implement secure mobile solutions.

description: Quick Response (QR) codes can be read by an imaging device such as a mobile device's camera or online. However, they pose a security risk. In this project, you create and use QR codes.

INTRODUCTION

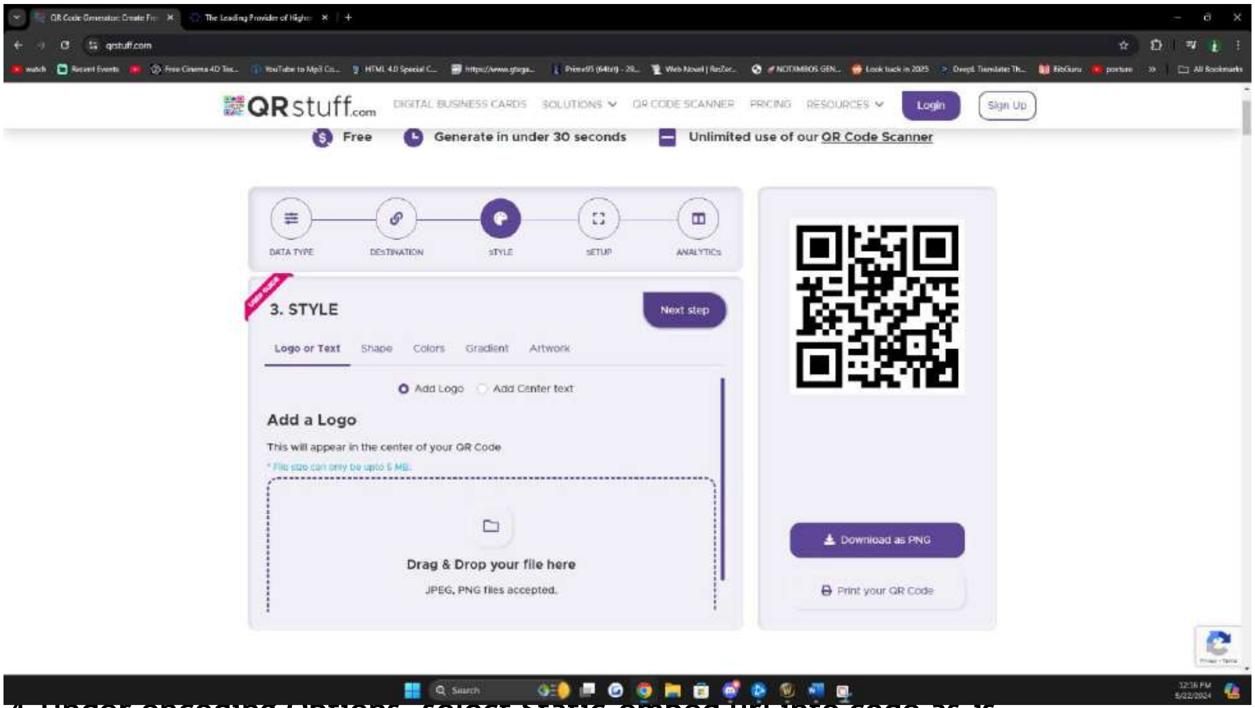
Quick Response codes are an easy way to deliver a URL or link to someone else with just a scan of their phones camera or a QR code reading app. However, there are many vulnerabilities with this such as "Quishing" which SecurityHQ (2023) describes as, tricking organizations into scanning a QR code to an impersonating fake website. (Thakkar, Kurkure, C Barlow, 2023) **Even through convenience, threat actors can slip their way through the cracks to take advantage of the technology.**

1. **Use your web browser to go to www.qrstuff.com. (If you are no longer able to access the program through this URL, use a search engine to search for "Qrstuff.")**



2. First create a QR code. Under Data Type, be sure that Website URL is selected.

3. Under Content, enter the URL www.cengage.com. Watch how the Qr code Preview changes as you type.



Free   Generate in under 30 seconds   Unlimited use of our QR Code Scanner

3. STYLE

● Add Logo ○ Add Center text

Add a Logo

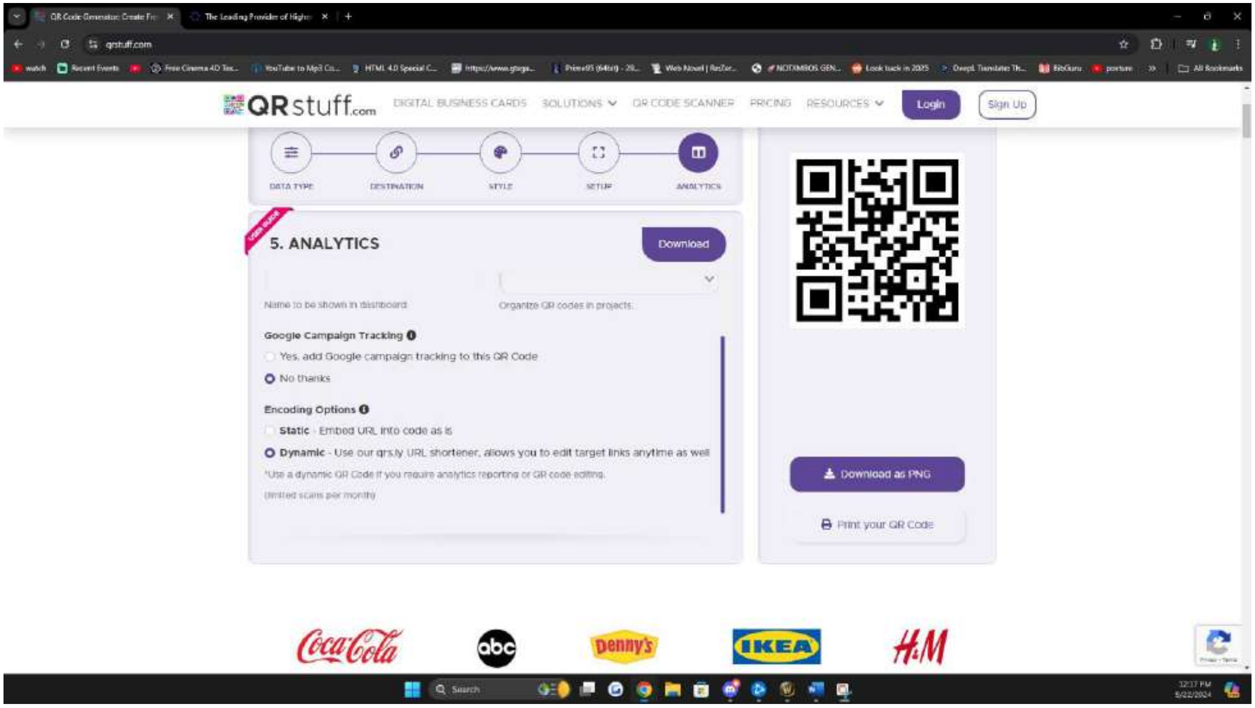
This will appear in the center of your QR Code

* File size can only be upto 5 MB.

Drag & Drop your file here

JPEG, PNG files accepted.

4. Under encoding Options, select Static-embed url into code as-is.



5. ANALYTICS

Name to be shown in dashboard

Organize QR codes in projects

Google Campaign Tracking

○ Yes, add Google campaign tracking to this QR Code

● No thanks

Encoding Options

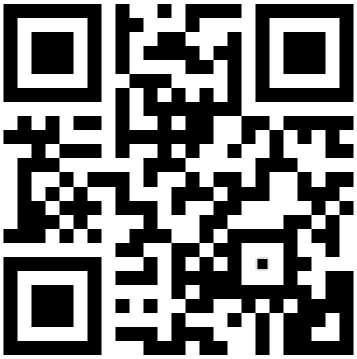
○ Static - Embed URL into code as is

● Dynamic - Use our qrs.ly URL shortener, allows you to edit target links anytime as well

*Use a dynamic QR Code if you require analytics reporting or QR code editing.

Unlimited scans per month

5. Under Qr code Preview, click Download Qr COde to download an image of the QR code.



6. Navigate to the location of the download and open the image. Is there anything you can tell by looking at this code? How could threat actors use this to their advantage? Where could malicious QR codes be used? Is there any protection for the user when using QR codes?

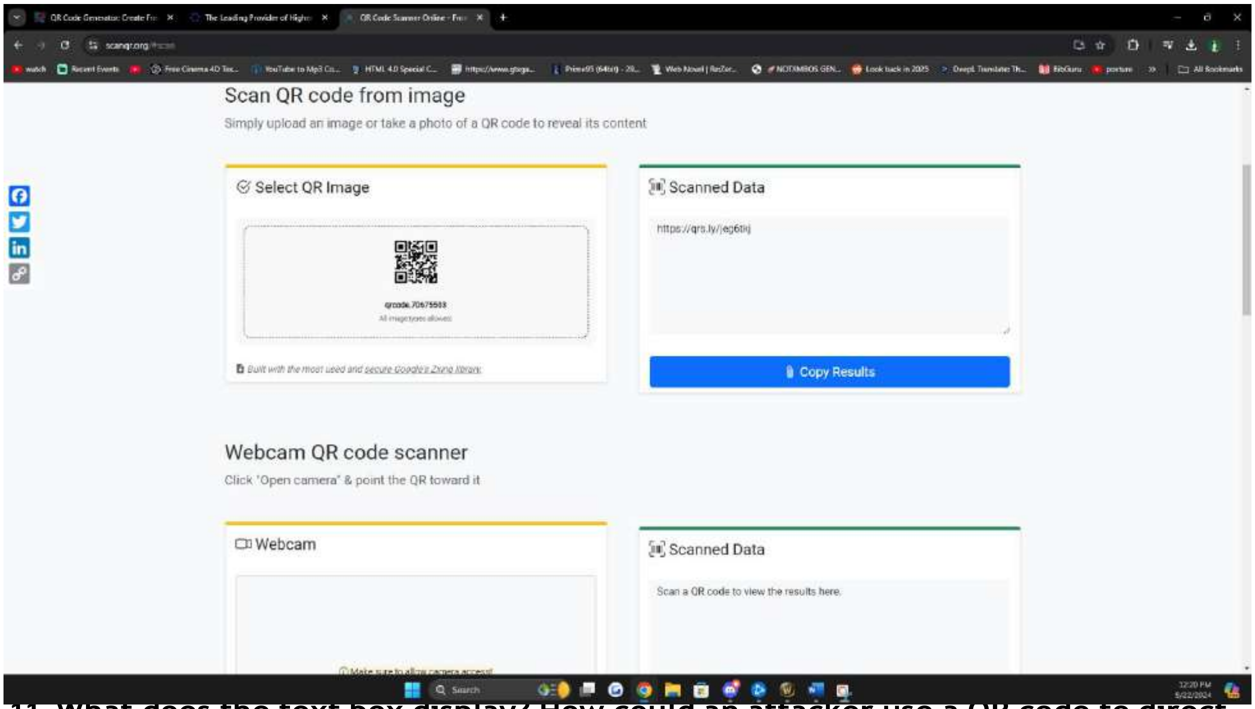
Malicious QR codes can lead to phishing websites designed to steal personal information or login credentials. All QR codes look very similar. If possible, check the URL encoded in the QR code to ensure it's legitimate.

7. Now use an online reader to interpret the QR code. Use your web browser to go to blog.qr4.nl/Online-QrCode_decoder.aspx. (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine and search for "Free Online QR Code Reader.")

8. Click Choose File.

G. Navigate to the location of the QR code that you downloaded on your computer and click Open.

10. **Click upload.**



Scan QR code from image

Simply upload an image or take a photo of a QR code to reveal its content

Select QR Image

qrcode.70675503

All image types allowed

Built with the most used and secure Google's Zxing library.

Scanned Data

https://qrs.ly/jeg6tkj

Copy Results

Webcam QR code scanner

Click 'Open camera' & point the QR toward it

Webcam

Scanned Data

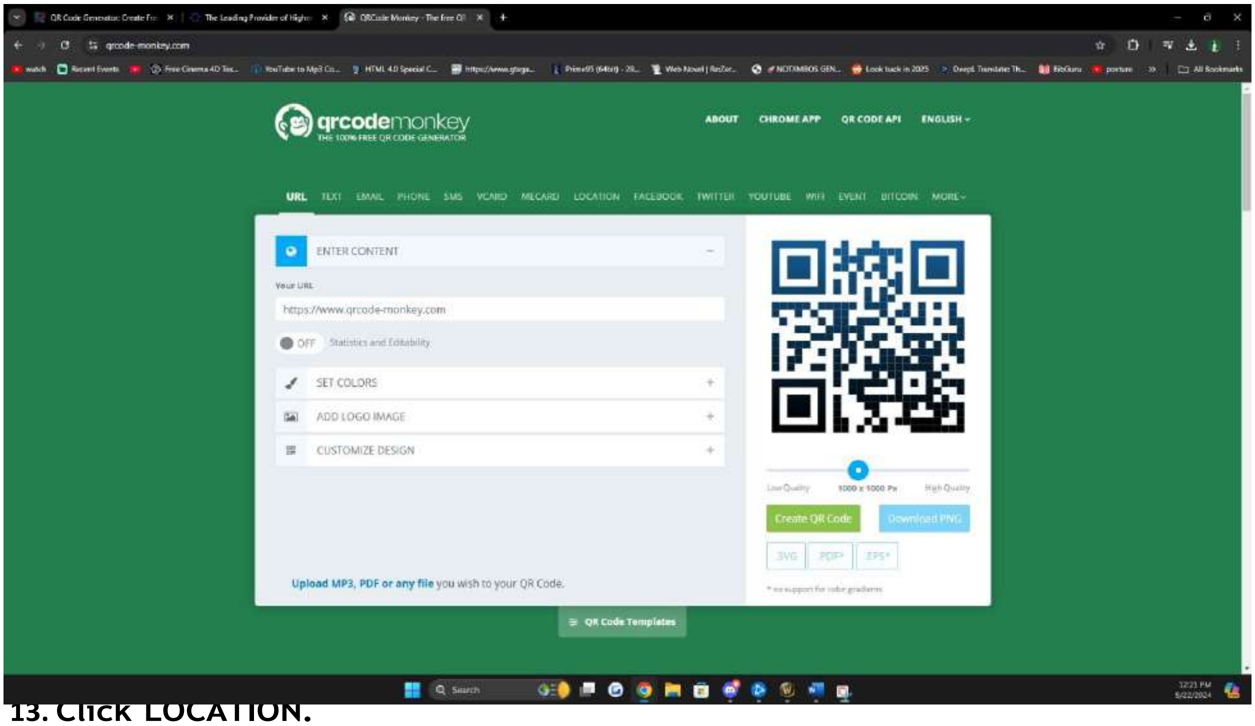
Scan a QR code to view the results here.

Make sure to allow camera access!

11. **What does the text box display? How could an attacker use a QR code to direct a victim to a malicious website?**

<u>It returns the URL encoded into the QR Code. Most of the time you don't really look at the link and you just click the qr code on your phone's camera.</u>

12. Use your web browser to go to qrcode-monkey.com. (If you are no longer able to access
the program through this URL, use a search engine to search for "qrcodemonkey.")



Your URL
https://www.qrcode-monkey.com

OFF Statistics and Editability

Upload MP3, PDF or any file you wish to your QR Code.

13. Click LOCATION.

14. On the map, drag the pointer to an address with which you are familiar.
Note how the latitude and longitude change.

15. Click Create Qr Code.

16. Click download pnG to download this QR code to your computer.

17. Navigate to the location of the download and open the image. How does it look different from the previous QR code? Is there anything you can tell by looking at this code?

You can tell nothing at all and it looks basically the same as the other QR code.

18. Use your web browser to return to blog.qr4.nl/Online-Qr-Code_decoder.aspx.

1G. Click Choose File.

20. Navigate to the location of the map QR code that you downloaded on your computer and click Open.

21. Click upload.

22. In the text box, a URL will be displayed. Paste this URL into a web browser.

23. What does the browser display? How could an attacker use this for a malicious attack?

Well it made a QR code of a location on google maps that I clicked. I don’t think there’s
anything to use off of this.

24. Return to www.qrstuff.com.

25. Click each option under dATA TyPe to view the different items that can be created by a QR code. Select three and indicate how they could be used by an attacker.

Download malicious apps

Direct you to social media

Text file

26. Close all windows.

Case Project 4-3: Application Patch Management

Select four third-party applications (not OSs) that you frequently use. How does each of them address patch management? Visit their websites to determine how they alert users to new vulnerabilities. Are the patch management systems adequate? Should patch management be required of all third-party applications? What are the advantages? What are the disadvantages? Write a one-page paper on your findings

INTRODUCTION

Most supported by the organization applications provide application patch management. From IBM, patch management is the process of applying vendor-issued updates to close any vulnerabilities and optimize the application. (International Business Machines, n.d.) As exploiters take advantage of applications, it is the responsibility of the vendor to address these problems and the process of maintaining their applications is what makes application patch management important for consumers.

The first application I frequently use is Google Chrome as a web browser. They suggest users to have auto-update enabled, version pinning which downloads updates when the user is ready, and fully manual updates. They are very adequate for Google Chrome as the critical ones are forcefully pushed, while the not so important ones aren't and are manual. They don't alert people of vulnerabilities.

The second application I frequently use is the Microsoft Office 365 suite. They automatically apply updates without the user even knowing, which is configurable. They also have the Office Deployment tool for organizations to configure their devices time to update so it doesn't disrupt their workflow. Microsoft is adequately handling their patch management for their Office 365 applications. They don't reveal any security vulnerabilities however have it set up to automatically report them from the application silently.

The third application I frequently use is Steam for gaming purposes. Steam handles their patch management by checking for an update before the user is allowed to get on the platform and if prompts the user to restart the client if there is an update available. Steam does not report security vulnerabilities to their users, like the other applications the news sites do that. Steam is adequately handling their application patch management.

The last application I frequently use is Spotify for music. Spotify handles their patch management by letting users update whenever they want on mobile devices, I think the desktop versions are auto-updates though. Spotify is open about their vulnerabilities and talks about their vulnerability reporting system on their website. Spotify is somewhat adequately handling their patch management, you really never have to update it on your phone so it can have many vulnerabilities lurking.

Application patch management should not be required by all third-party applications. It should only be required for third-party applications that need it and are online services where vulnerabilities are more prominent. Any application that had the ability to connect to the internet at some point, so all of the Adobe applications for example. It is ultimately up to the creator at the end of the day.

Some advantages of it from SentinelOne (2023) include, “Patch management helps establish a strong foundation for enhanced security, risk mitigation, regulatory compliance, cost savings, and improved operational continuity. By prioritizing and implementing effective patch management practices, organizations can strengthen their cybersecurity defenses and protect their data, reputation, and bottom line.” (SentinelOne, 2023) . Patch management keeps applications secure and functional for many years if the management is continued.

Some disadvantages of it from Scappman (2022) include, the time-consumption involved, lack of IT inventory management, no desire to deploy the patches, patch failures, and vulnerability management. (Scappman, 2022) The process of diagnosing, testing, and applying the patches leads to a time management problem. There are also patch failures where applying the fixes, breaks something else, or could disable the program temporarily. Thinking about longevity, having to apply patches for an application no one uses 20 years down the line is really demotivating and lacks a benefit to the company. The cycle continues with every fix and there’s always another problem to fix, it’s just a matter of worth to the company and forcing it on them is entirely up to them.

References

International Business Machines. (n.d.). *What is patch management?* Retrieved from IBM: https://www.ibm.com/topics/patch-management

Scappman. (2022, August 5). *Top 5 Challenges of patch management*. Retrieved from Scappman: https://www.scappman.com/post/top-5-challenges-of-patch-management

SentinelOne. (2023, September 29). *What is Patch Management? Working and Benefits*. Retrieved from SentinelOne: https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is- patch-management/

Thakkar, D., Kurkure, N., C Barlow, E. (2023, October). *QR Code Vulnerabilities: Dissecting New Techniques Seen in the Wild*. Retrieved from SecurityHQ: https://www.securityhq.com/blog/qr-code-vulnerabilities-dissecting-new-techniques- seen-in-the-wild

VirusTotal. (n.d.). *VirusTotal - Home*. Retrieved from VirusTotal: https://www.virustotal.com/

Assignment 3 - Hands On

Sam Peller

October 10, 2024

ISM 4323

Project 6-4: Using Microsoft’s Encrypting File System (EFS)

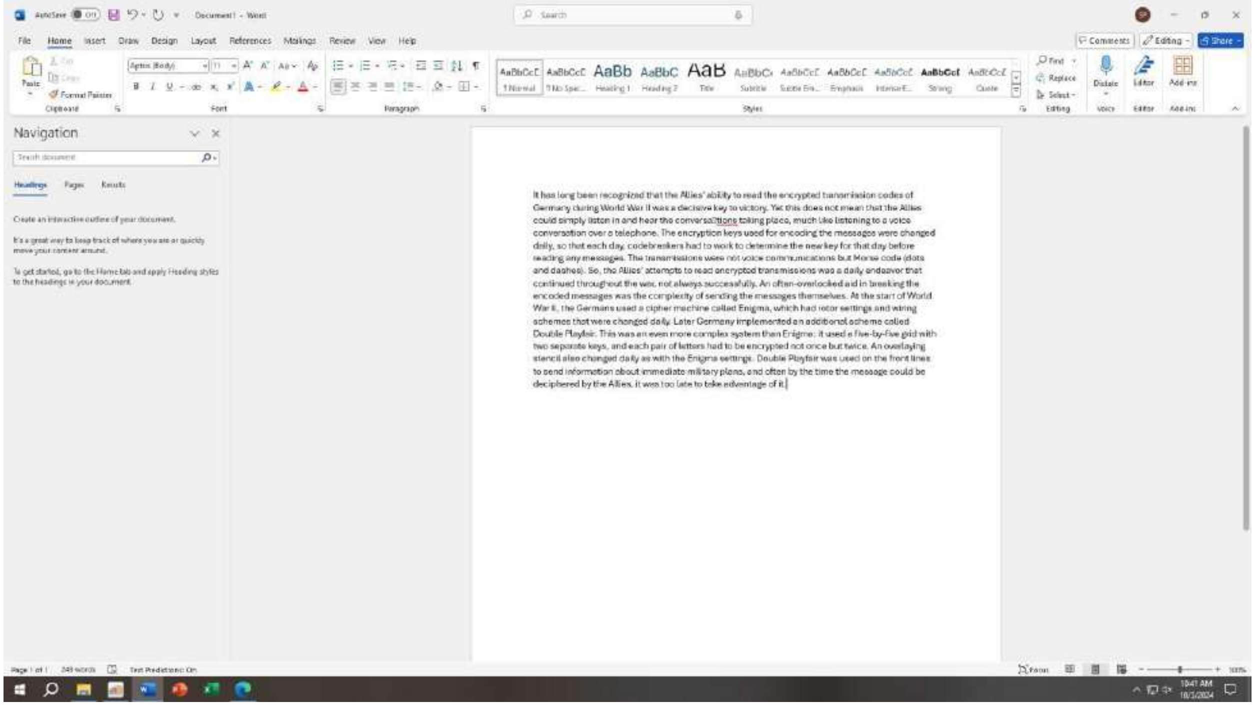
Time Required: 20 minutes

Objective: Given a scenario, implement host or application security solutions. Description: Microsoft’s Encrypting File System (EFS) is a cryptography system for Windows releases that use the Windows NT file system (NTFS). Because EFS is tightly integrated with the file system, file encryption and decryption are transparent to the user. In this project, you will turn on and use EFS.

INTRODUCTION

The Encrypted File System (EFS) is a security feature in Windows that enhances file protection by encrypting individual files on NTFS volumes using a public-key cryptography system. While Windows access control typically protects files from unauthorized access, according to Microsoft (2023) EFS adds an extra layer of security, particularly useful if a device containing sensitive information is lost or stolen (Microsoft, 2023). By going to the properties of a file and going into the advanced option you can simply turn it on.

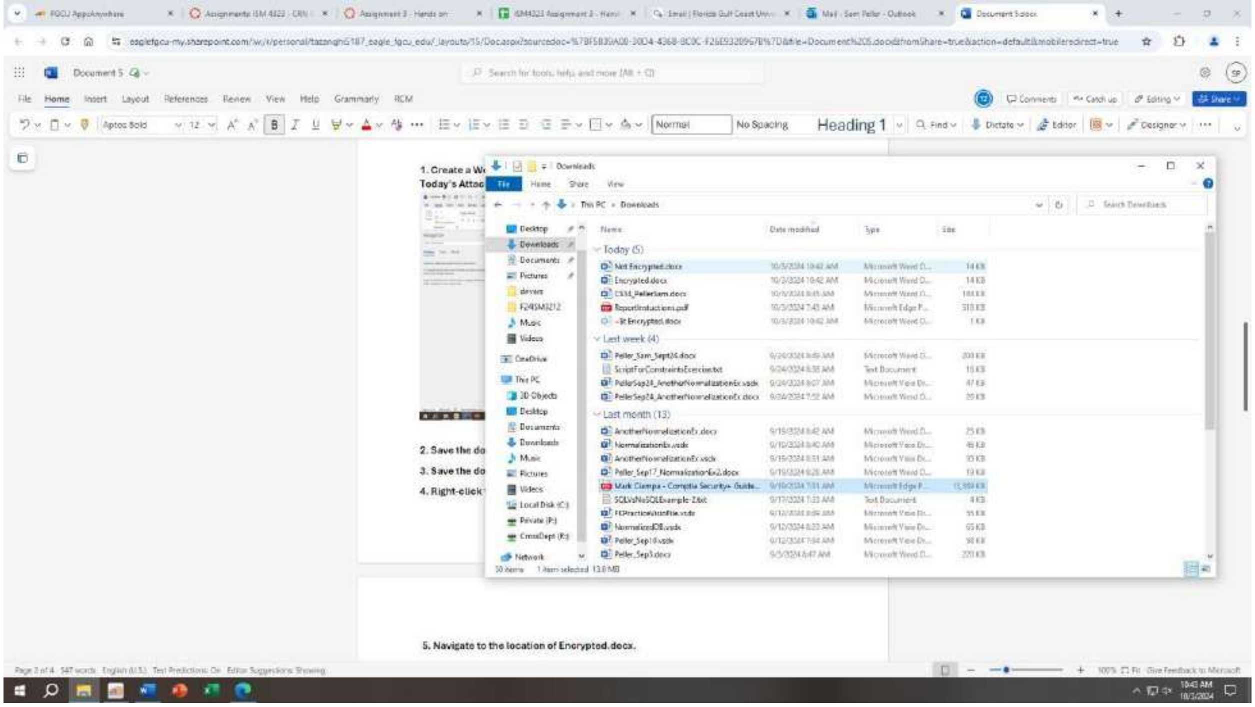
1. **Create a Word document with the contents of the first two paragraphs under Today's Attacks and Defenses on the first page of this module.**



It has long been recognized that the Allies' ability to read the encrypted transmission codes of Germany during World War II was a decisive key to victory. Yet this does not mean that the Allies could simply listen in and hear the conversations taking place, much like listening to a voice conversation over a telephone. The encryption keys used for encoding the messages were changed daily, so that each day, codebreakers had to work to determine the new key for that day before reading any messages. The transmissions were not voice communications but Morse code (dots and dashes). So, the Allies' attempts to read encrypted transmissions was a daily endeavor that continued throughout the war, not always successfully. An often-overlooked aid in breaking the encoded messages was the complexity of sending the messages themselves. At the start of World War II, the Germans used a cipher machine called Enigma, which had rotor settings and wiring schemes that were changed daily. Later Germany implemented an additional scheme called Double Playfair. This was an even more complex system than Enigma: it used a five-by-five grid with two separate keys, and each pair of letters had to be encrypted not once but twice. An overlaying stencil also changed daily as with the Enigma settings. Double Playfair was used on the front lines to send information about immediate military plans, and often by the time the message could be deciphered by the Allies, it was too late to take advantage of it.

2. **Save the document as Encrypted.docx.**

3. Save the document again as Not Encrypted.docx.



Downloads

This PC › Downloads

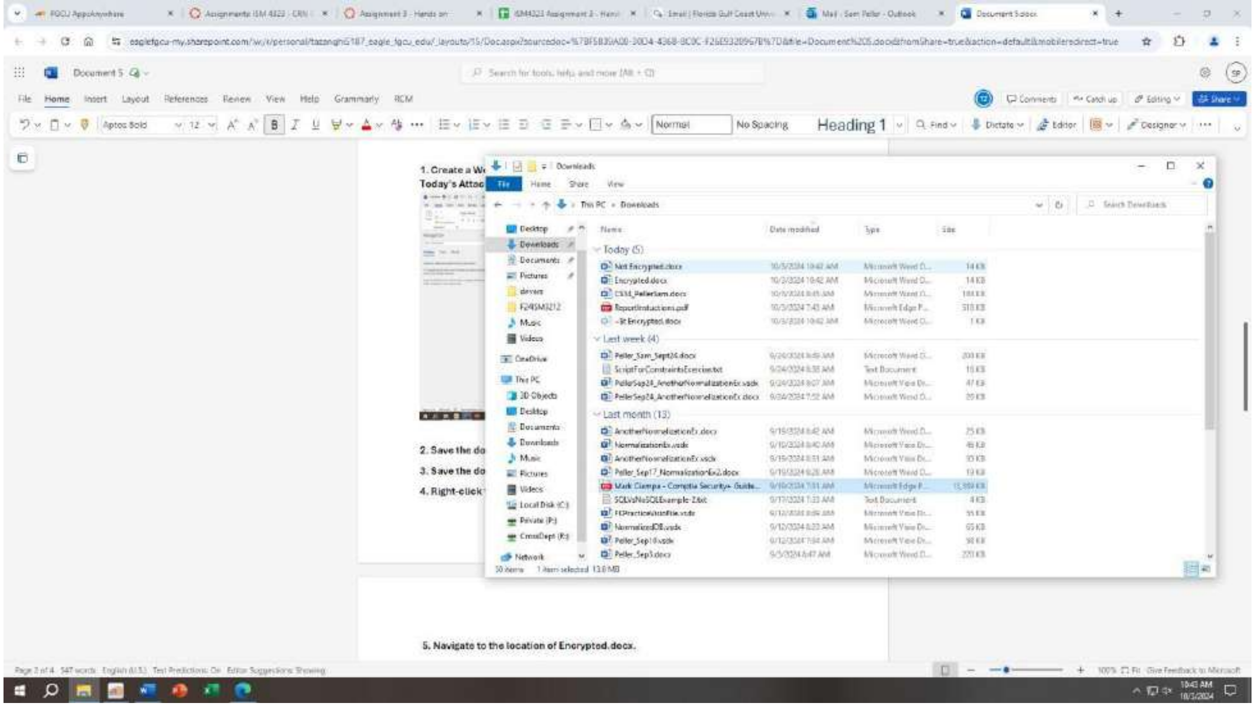
Name	Date modified	Type	Size
Today (5)			
Not Encrypted.docx	10/3/2024 10:42 AM	Microsoft Word D...	14 KB
Encrypted.docx	10/3/2024 10:42 AM	Microsoft Word D...	14 KB
CS34_PellerSam.docx	10/3/2024 8:45 AM	Microsoft Word D...	188 KB
ReportInstructions.pdf	10/3/2024 7:43 AM	Microsoft Edge P...	510 KB
~$t Encrypted.docx	10/3/2024 10:42 AM	Microsoft Word D...	1 KB
Last week (4)			
Peller_Sam_Sept24.docx	9/24/2024 8:49 AM	Microsoft Word D...	200 KB
ScriptForConstraintsExercise.txt	9/24/2024 8:38 AM	Text Document	15 KB
PellerSep24_AnotherNormalizationEx.vsdx	9/24/2024 8:07 AM	Microsoft Visio Dr...	47 KB
PellerSep24_AnotherNormalizationEx.docx	9/24/2024 7:52 AM	Microsoft Word D...	20 KB
Last month (13)			
AnotherNormalizationEx.docx	9/19/2024 8:42 AM	Microsoft Word D...	25 KB
NormalizationEx.vsdx	9/10/2024 8:40 AM	Microsoft Visio Dr...	45 KB
AnotherNormalizationEx.vsdx	9/19/2024 8:31 AM	Microsoft Visio Dr...	33 KB
Peller_Sep17_NormalizationEx2.docx	9/19/2024 8:26 AM	Microsoft Word D...	19 KB
Mark Ciampa - Comptia Security+ Guide...	9/10/2024 7:31 AM	Microsoft Edge P...	13,989 KB
SQLvsNoSQLExample-2.txt	9/17/2024 1:33 AM	Text Document	4 KB
FKPracticeVisioFile.vsdx	9/12/2024 8:06 AM	Microsoft Visio Dr...	55 KB
NormalizedDB.vsdx	9/12/2024 8:23 AM	Microsoft Visio Dr...	65 KB
Peller_Sep10.vsdx	9/12/2024 7:54 AM	Microsoft Visio Dr...	98 KB
Peller_Sep3.docx	9/5/2024 8:47 AM	Microsoft Word D...	220 KB

50 items 1 item selected 13.6 MB

5. Navigate to the location of Encrypted.docx.

4. Right-click the Start button, and then click File Explorer.

5. Navigate to the location of Encrypted.docx.



Downloads

This PC › Downloads

Name	Date modified	Type	Size
Today (5)			
Not Encrypted.docx	10/3/2024 10:42 AM	Microsoft Word D...	14 KB
Encrypted.docx	10/3/2024 10:42 AM	Microsoft Word D...	14 KB
CS34_PellerSam.docx	10/3/2024 8:45 AM	Microsoft Word D...	188 KB
ReportInstructions.pdf	10/3/2024 7:43 AM	Microsoft Edge P...	510 KB
~$t Encrypted.docx	10/3/2024 10:42 AM	Microsoft Word D...	1 KB
Last week (4)			
Peller_Sam_Sept24.docx	9/24/2024 8:49 AM	Microsoft Word D...	200 KB
ScriptForConstraintsExercise.txt	9/24/2024 8:38 AM	Text Document	15 KB
PellerSep24_AnotherNormalizationEx.vsdx	9/24/2024 8:07 AM	Microsoft Visio Dr...	47 KB
PellerSep24_AnotherNormalizationEx.docx	9/24/2024 7:52 AM	Microsoft Word D...	20 KB
Last month (13)			
AnotherNormalizationEx.docx	9/19/2024 8:42 AM	Microsoft Word D...	25 KB
NormalizationEx.vsdx	9/10/2024 8:40 AM	Microsoft Visio Dr...	45 KB
AnotherNormalizationEx.vsdx	9/19/2024 8:31 AM	Microsoft Visio Dr...	33 KB
Peller_Sep17_NormalizationEx2.docx	9/19/2024 8:26 AM	Microsoft Word D...	19 KB
Mark Ciampa - Comptia Security+ Guide...	9/10/2024 7:31 AM	Microsoft Edge P...	13,989 KB
SQLvsNoSQLExample-2.txt	9/17/2024 1:33 AM	Text Document	4 KB
FKPracticeVisioFile.vsdx	9/12/2024 8:06 AM	Microsoft Visio Dr...	55 KB
NormalizedDB.vsdx	9/12/2024 8:23 AM	Microsoft Visio Dr...	65 KB
Peller_Sep10.vsdx	9/12/2024 7:54 AM	Microsoft Visio Dr...	98 KB
Peller_Sep3.docx	9/5/2024 8:47 AM	Microsoft Word D...	220 KB

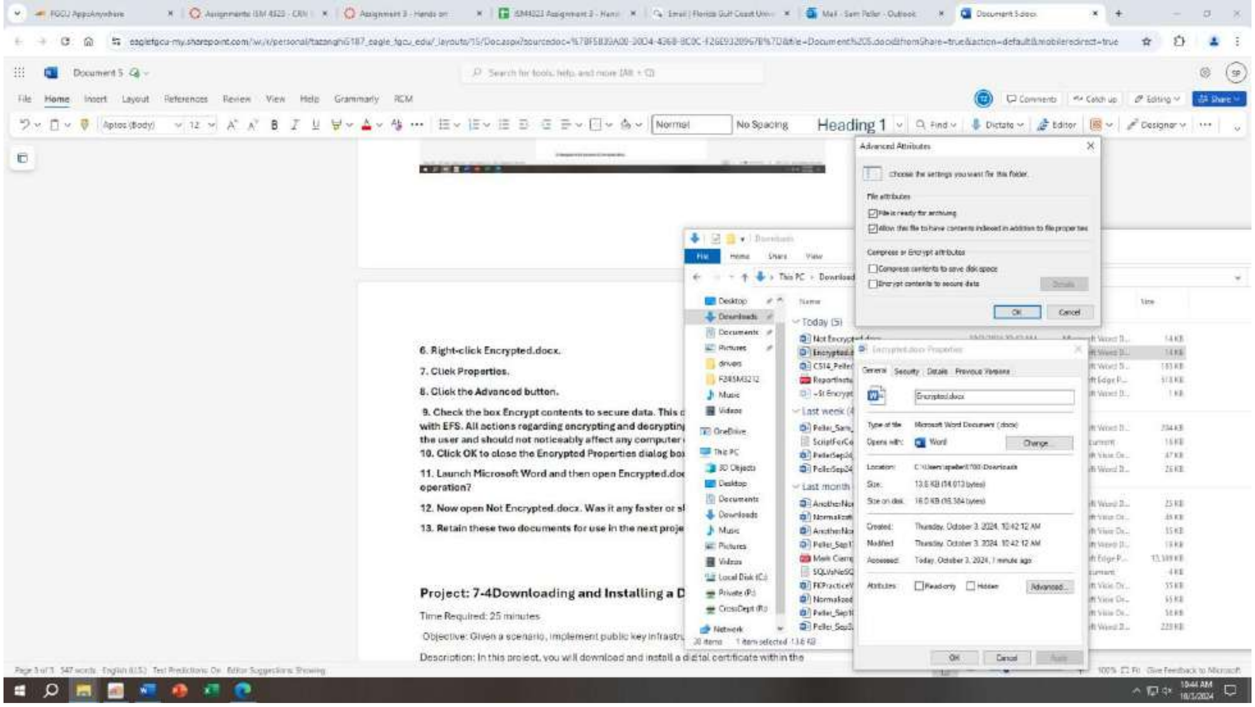
50 items 1 item selected 13.6 MB

5. Navigate to the location of Encrypted.docx.

6. Right-click Encrypted.docx.

7. Click Properties.

8. Click the Advanced button.



6. Right-click Encrypted.docx.

7. Click Properties.

8. Click the Advanced button.

9. Check the box Encrypt contents to secure data. This c
with EFS. All actions regarding encrypting and decryptin
the user and should not noticeably affect any computer
10. Click OK to close the Encrypted Properties dialog bo

11. Launch Microsoft Word and then open Encrypted.do
operation?

12. Now open Not Encrypted.docx. Was it any faster or s

13. Retain these two documents for use in the next proje

Project: 7-4Downloading and Installing a D

Time Required: 25 minutes

Objective: Given a scenario, implement public key infrastru

Description: In this project, you will download and install a digital certificate within the

Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☐ Encrypt contents to secure data

Encrypted.docx Properties

Type of file: Microsoft Word Document (.docx)

Opens with: Word

Size: 13.6 KB (14,013 bytes)

Size on disk: 16.0 KB (16,384 bytes)

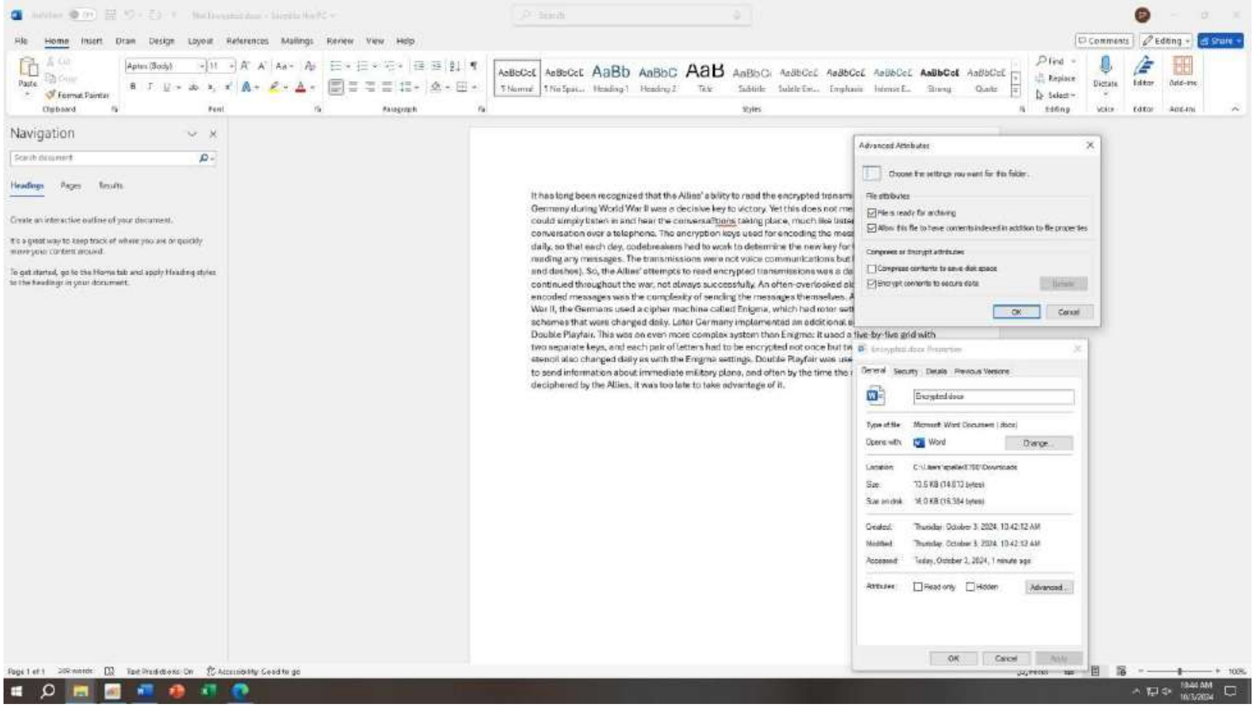
Created: Thursday, October 3, 2024, 10:42:12 AM

Modified: Thursday, October 3, 2024, 10:42:12 AM

Accessed: Today, October 3, 2024, 1 minute ago

Attributes: ☐ Read-only ☐ Hidden

G. Check the box Encrypt contents to secure data. This document is now protected with EFS. All actions regarding encrypting and decrypting the file are transparent to the user and should not noticeably affect any computer operations. Click OK.



It has long been recognized that the Allies' ability to read the encrypted transmi
Germany during World War II was a decisive key to victory. Yet this does not me
could simply listen in and hear the conversaitions taking place, much like liste
conversation over a telephone. The encryption keys used for encoding the mess
daily, so that each day, codebreakers had to work to determine the new key for
reading any messages. The transmissions were not voice communications but
and dashes). So, the Allies' attempts to read encrypted transmissions was a de
continued throughout the war, not always successfully. An often-overlooked al
encoded messages was the complexity of sending the messages themselves. A
War II, the Germans used a cipher machine called Enigma, which had rotor set
schemes that were changed daily. Later Germany implemented an additional s
Double Playfair. This was an even more complex system than Enigma: It used a five-by-five grid with
two separate keys, and each pair of letters had to be encrypted not once but tw
stencil also changed daily as with the Enigma settings. Double Playfair was use
to send information about immediate military plans, and often by the time the
deciphered by the Allies, it was too late to take advantage of it.

Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

Encrypted.docx Properties

Type of file: Microsoft Word Document (.docx)

Opens with: Word

Size: 13.5 KB (14,013 bytes)

Size on disk: 16.0 KB (16,384 bytes)

Created: Thursday, October 3, 2024, 10:42:12 AM

Modified: Thursday, October 3, 2024, 10:42:12 AM

Accessed: Today, October 3, 2024, 1 minute ago

Attributes: ☐ Read-only ☐ Hidden

10. Click OK to close the Encrypted Properties dialog box.

11. Launch Microsoft Word and then open Encrypted.docx. Was there any delay in the operation? There wasn’t any noticeable difference between opening the two files.

12. Now open Not Encrypted.docx. Was it any faster or slower?

There wasn’t any noticeable difference between opening the two files.

13. Retain these two documents for use in the next project. Close Word

Case Project 6-6: One-Time Pad (OTP) Research

Use the Internet to research OTPs: who was behind the initial idea, when they were first used, in what applications they were found, how they are used today, and other relevant information. Then visit an online OTP creation site such as www.braingle.com/brainteasers/codes/onetimepad.php and practice creating your own ciphertext with OTP. If possible, exchange your OTPs with other students to see how you might try to break them. Would it be practical to use OTPs? Why or why not? Write a one-page paper on your findings

INTRODUCTION

The one-time pad (OTP) is a classic encryption method celebrated for its theoretical unbreakability, relying on the use of a pre-shared key that is longer than the message itself as a double-edged sword. Some of its applications from ReasonLabs (2023), describe it as used in some antivirus programs to securely store and transmit sensitive data, such as encryption keys and decryption algorithms (ReasonLabs, 2023). If all electronics went offline for a period in time, the one-time pad would be a great method to send encrypted messages in times of need.

A one-time pad is an encryption technique that is supposed to be uncrackable but requires the use of a pre-shared key larger than the message being sent. According to Crypto Museum (2023), the initial idea was by banker Frank Miller which was later reinvented. It was first used by agents of the former Soviet Union during the 1960s (Crypto Museum, 2023). It's a one-time pad because it's a booklet of either letters or numbers stapled together and after usage is destroyed. They can be hidden inside small objects and are supposed to be concealable. According to Reason Labs (2023), the keys are generally not practical for everyday use but are still sometimes used for improved confidentiality in military or government communications, when used correctly it's considered unbreakable. (ReasonLabs, 2023)

To put it into practice, Braingle offers a simulator where to encipher a message, each letter of the plaintext is added to a corresponding letter from the one-time pad using their positions in the alphabet (A=1, B=2, etc.). After adding, 1 is subtracted from the result. If the sum exceeds 26, it wraps around the alphabet. To decipher, each letter of the ciphertext is subtracted from the corresponding one-time pad letter. If the result is negative, it wraps around to the end of the alphabet (Braingle, n.d.). From the website, you are provided a one-time pad code, you first encipher the plaintext, then you get an enciphered message. You then decipher it, and get a new enciphered message, and encipher it to get the message.

As One-Time pads are considered unbreakable when done correctly, they aren't practical to use. The length of the pad must be as long as the message being encrypted and it is inconvenient for such long and unique keys each time. The sender and receiver need identical copies of the OTP and vulnerabilities in transmission as well as re-use is not suggested. On the bright side, OTPs needs to be truly random and doing it on a large scale would not be optimal. Manually decrypting a message with this system is inefficient and error prone. It is not suggested to use OTP's in general use and would recommend modern day encryption methods.

One-time pads also present significant logistical issues beyond key management. They require a secure and trusted channel for exchanging the pads themselves before any communication can begin, which can be difficult to maintain. Furthermore, if an adversary gains access to even part of the one-time pad, the security of the system collapses entirely. Unlike modern encryption methods that allow for secure key exchange over public channels (like RSA or

Diffie-Hellman), OTPs do not offer such flexibility. These factors make them less practical in modern digital communication environments, where scalability and ease of use are essential.

References

Braingle. (n.d.). *One-time Pad Cipher*. Retrieved from Braingle: https://www.braingle.com/brainteasers/codes/onetimepad.php#form

Crypto Museum. (2023). *One-Time Pad (OTP)*. Retrieved from Crypto Museum: https://www.cryptomuseum.com/crypto/otp/index.htm

Microsoft. (2023, January 12). *File Encryption*. Retrieved from Microsoft: https://learn.microsoft.com/en-us/windows/win32/fileio/file-encryption

ReasonLabs. (2023). *What is One-time pad?* Retrieved from Reason Labs: https://cyberpedia.reasonlabs.com/EN/pre-shared%20key.html

Project 7-4: Downloading and Installing a Digital Certificate

Time Required: 25 minutes

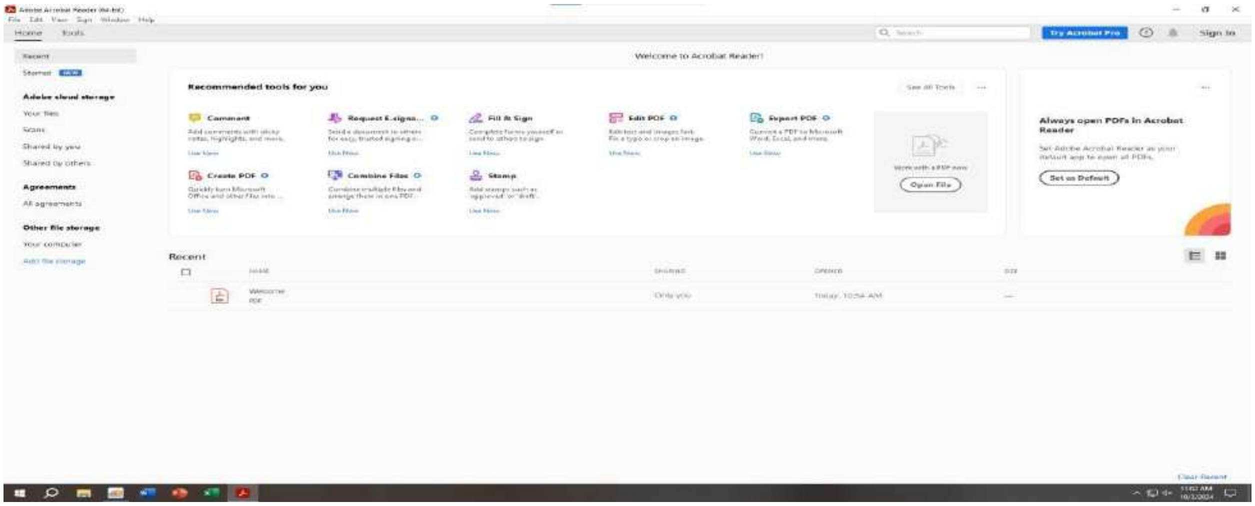
Objective: Given a scenario, implement public key infrastructure.

Description: In this project, you will download and install a digital certificate within the Adobe Acrobat Reader DC.

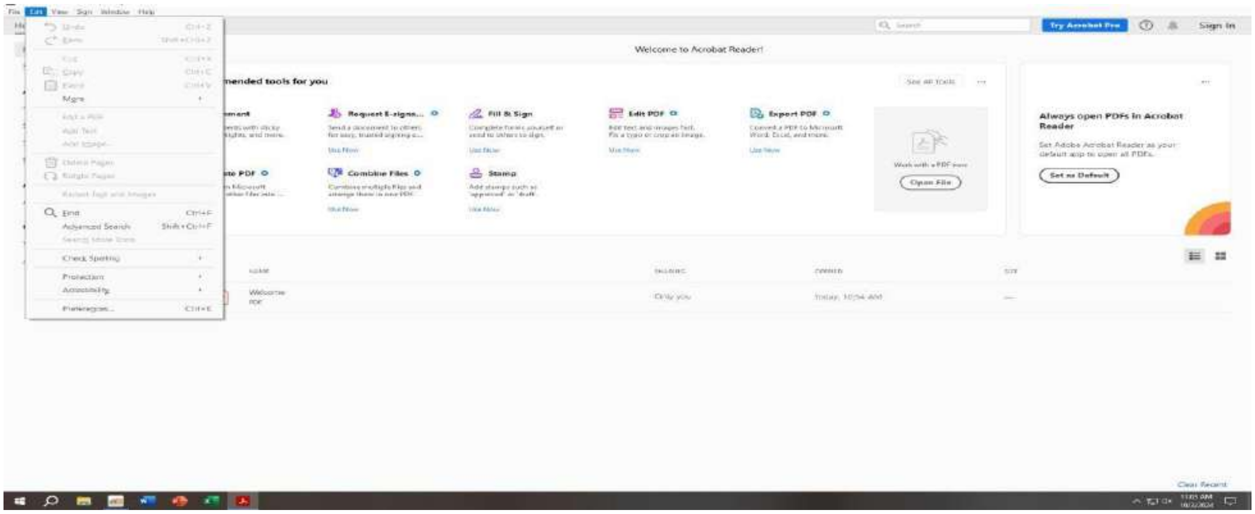
Introduction: Downloading and installing a digital certificate in Adobe Reader is a crucial step for enhancing the security and authenticity of your digital documents. A digital certificate serves as a virtual ID card, this allows users to sign, encrypt, and validate the integrity of files securely. This process not only helps protect sensitive information but also ensures that your electronic signatures are recognized and trusted by recipients.

1. Check to determine if Adobe Acrobat Reader DC or Adobe Acrobat Professional is installed on your computer. If so, you may skip these download and installation steps and go directly to Step 5.

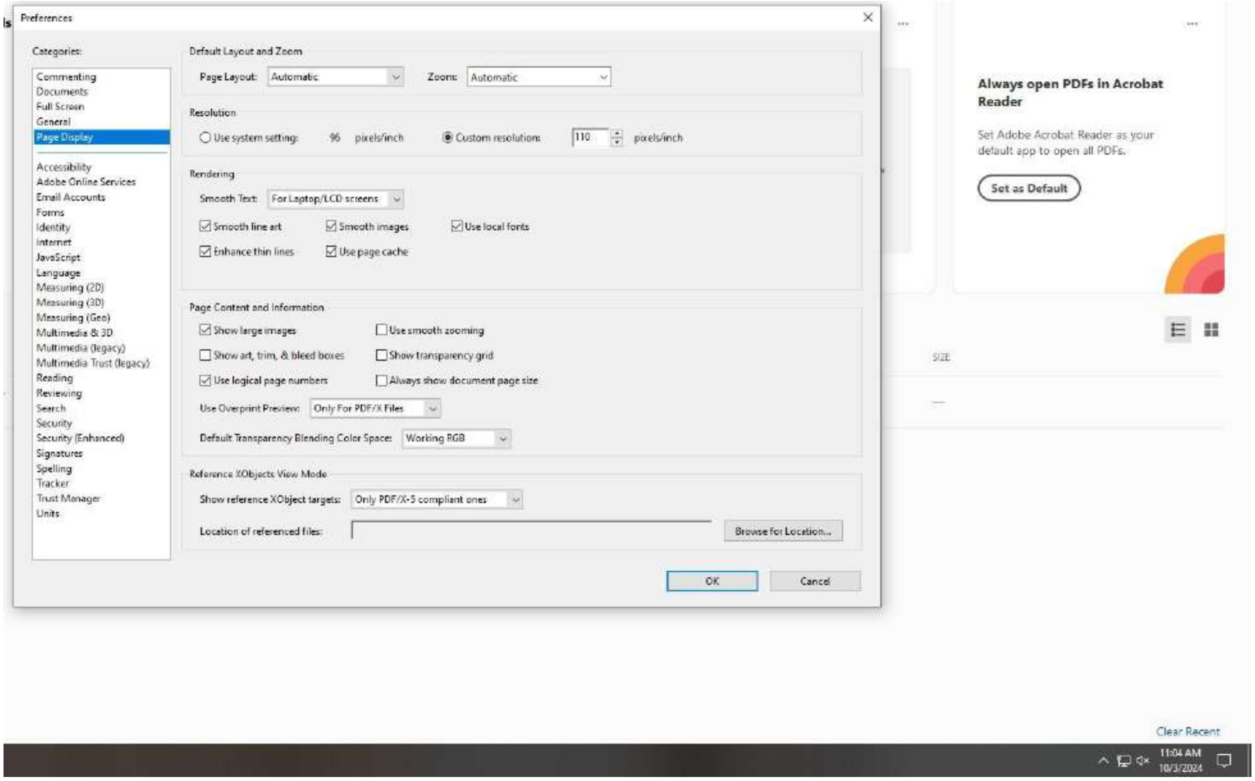
5. Launch Reader.



6. Click Edit.



7. Click Preferences.



Default Layout and Zoom

Page Layout: Automatic   Zoom: Automatic

Resolution

○ Use system setting: 96 pixels/inch   ● Custom resolution: 110 pixels/inch

Rendering

Smooth Text: For Laptop/LCD screens

☑ Smooth line art   ☑ Smooth images   ☑ Use local fonts

☑ Enhance thin lines   ☑ Use page cache

Page Content and Information

☑ Show large images   □ Use smooth zooming

□ Show art, trim, & bleed boxes   □ Show transparency grid

☑ Use logical page numbers   □ Always show document page size

Use Overprint Preview: Only For PDF/X Files

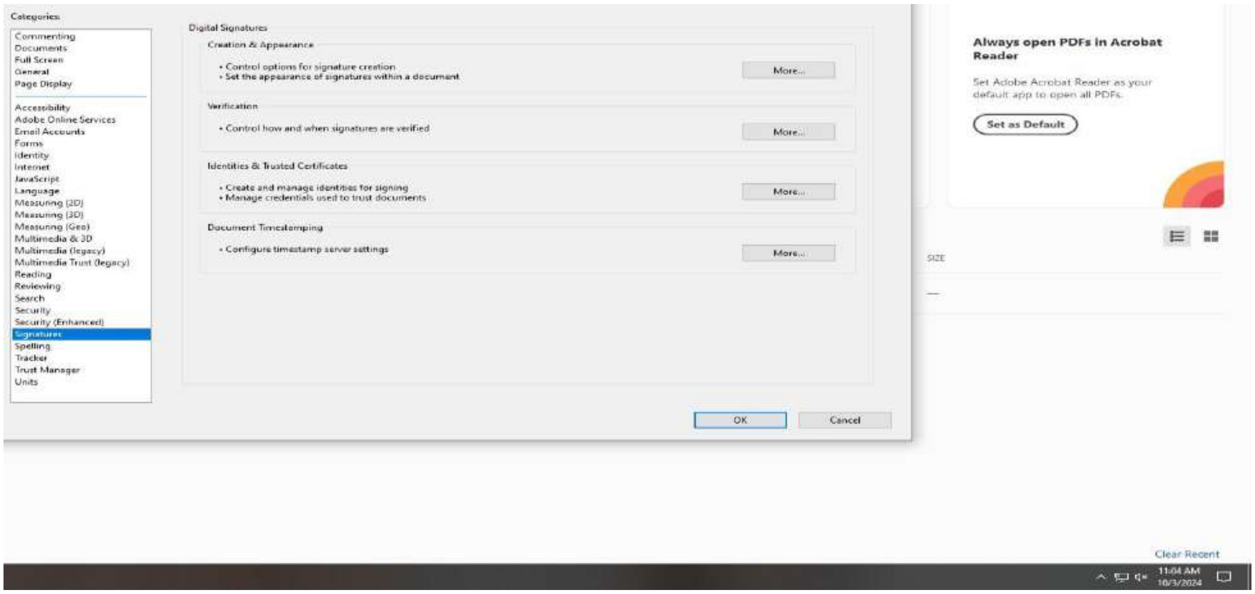
Default Transparency Blending Color Space: Working RGB

Reference XObjects View Mode

Show reference XObject targets: Only PDF/X-5 compliant ones

Location of referenced files:

8. Click Signatures.



Digital Signatures

Creation & Appearance

- Control options for signature creation
- Set the appearance of signatures within a document

Verification

- Control how and when signatures are verified

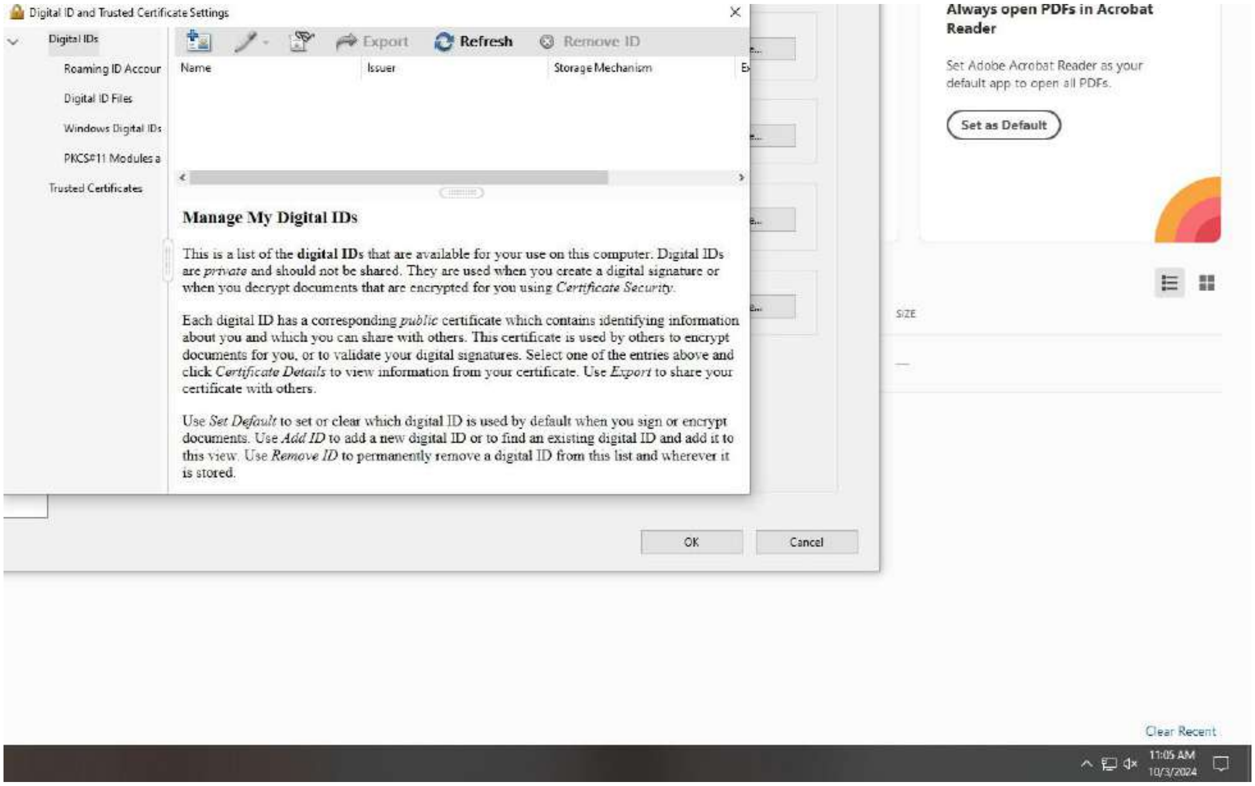
Identities & Trusted Certificates

- Create and manage identities for signing
- Manage credentials used to trust documents

Document Timestamping

- Configure timestamp server settings

9. Under Identities C Trusted Certificates, click More.



Manage My Digital IDs

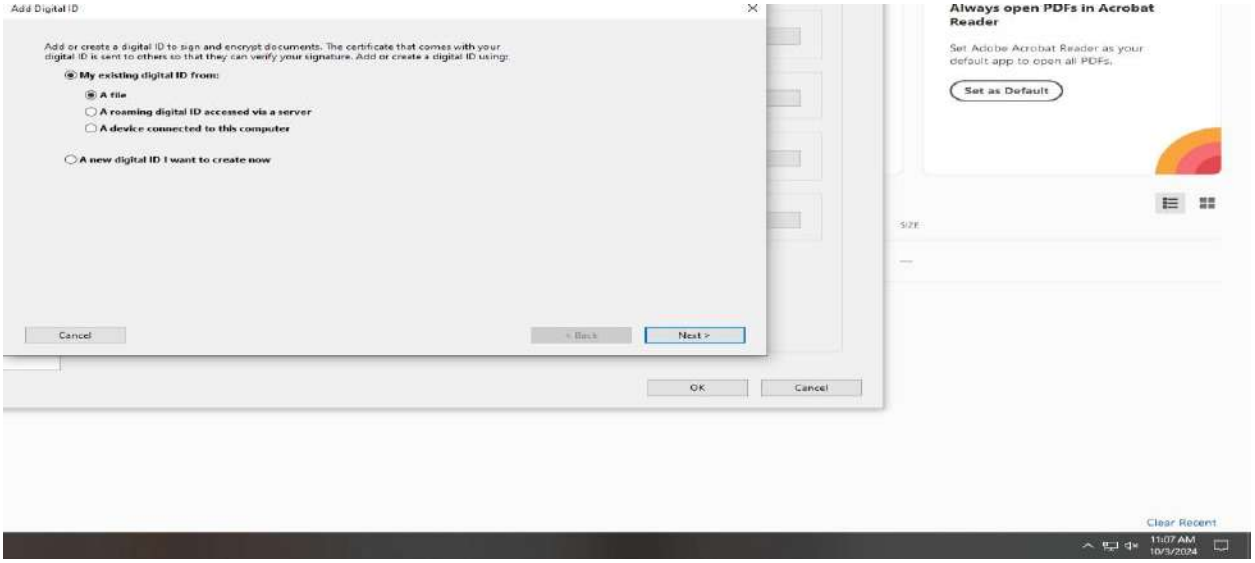
This is a list of the **digital IDs** that are available for your use on this computer. Digital IDs are *private* and should not be shared. They are used when you create a digital signature or when you decrypt documents that are encrypted for you using *Certificate Security*.

Each digital ID has a corresponding *public* certificate which contains identifying information about you and which you can share with others. This certificate is used by others to encrypt documents for you, or to validate your digital signatures. Select one of the entries above and click *Certificate Details* to view information from your certificate. Use *Export* to share your certificate with others.

Use *Set Default* to set or clear which digital ID is used by default when you sign or encrypt documents. Use *Add ID* to add a new digital ID or to find an existing digital ID and add it to this view. Use *Remove ID* to permanently remove a digital ID from this list and wherever it is stored.

10. In the left pane, click Digital IDs to display the menu choices, if necessary.

11. At the menu at the top of the main pane, click the Add ID icon (it is the first icon and has a plus sign).



Add Digital ID
Cancel
< Back
Next >
OK
Cancel
Always open PDFs in Acrobat Reader
Set Adobe Acrobat Reader as your default app to open all PDFs.
Set as Default
SIZE
Clear Recent
11:07 AM
10/3/2024

Add or create a digital ID to sign and encrypt documents. The certificate that comes with your digital ID is sent to others so that they can verify your signature. Add or create a digital ID using:

● My existing digital ID from:

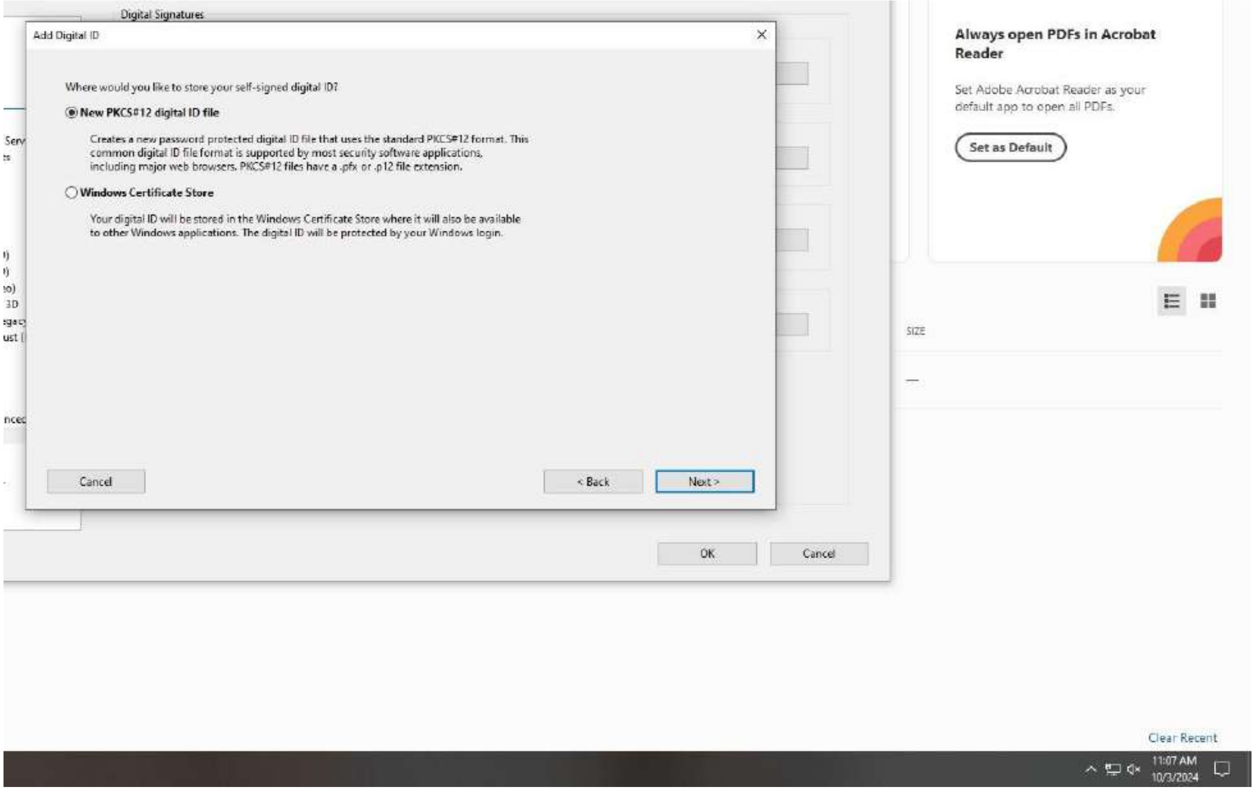
● A file

○ A roaming digital ID accessed via a server

○ A device connected to this computer

○ A new digital ID I want to create now

12. Click A new digital ID I want to create now. Click Next.



Where would you like to store your self-signed digital ID?

● New PKCS#12 digital ID file

Creates a new password protected digital ID file that uses the standard PKCS#12 format. This common digital ID file format is supported by most security software applications, including major web browsers. PKCS#12 files have a .pfx or .p12 file extension.

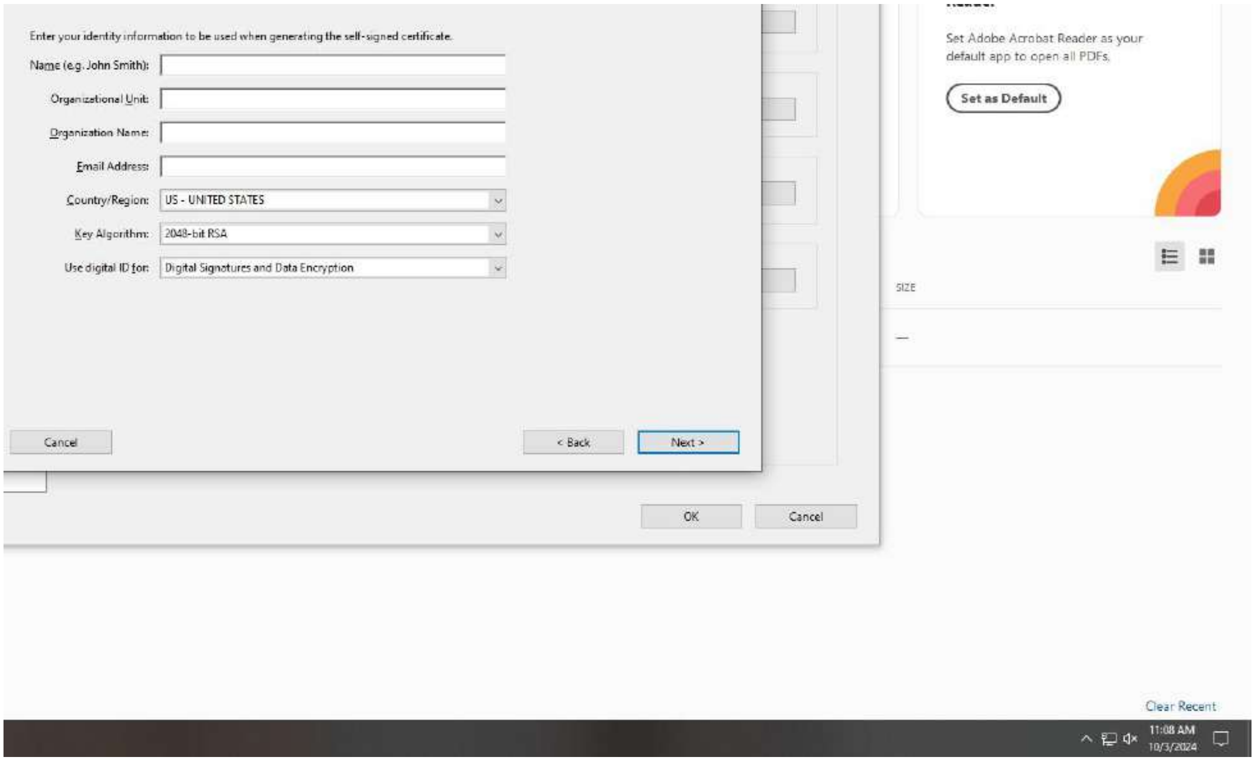
○ Windows Certificate Store

Your digital ID will be stored in the Windows Certificate Store where it will also be available to other Windows applications. The digital ID will be protected by your Windows login.

Always open PDFs in Acrobat Reader

Set Adobe Acrobat Reader as your default app to open all PDFs.

13. If necessary, click New PKCS#12 digital ID file. What is a PKCS#12? What type of file extension will it have? Click Next.



Enter your identity information to be used when generating the self-signed certificate.

Name (e.g. John Smith):

Organizational Unit:

Organization Name:

Email Address:

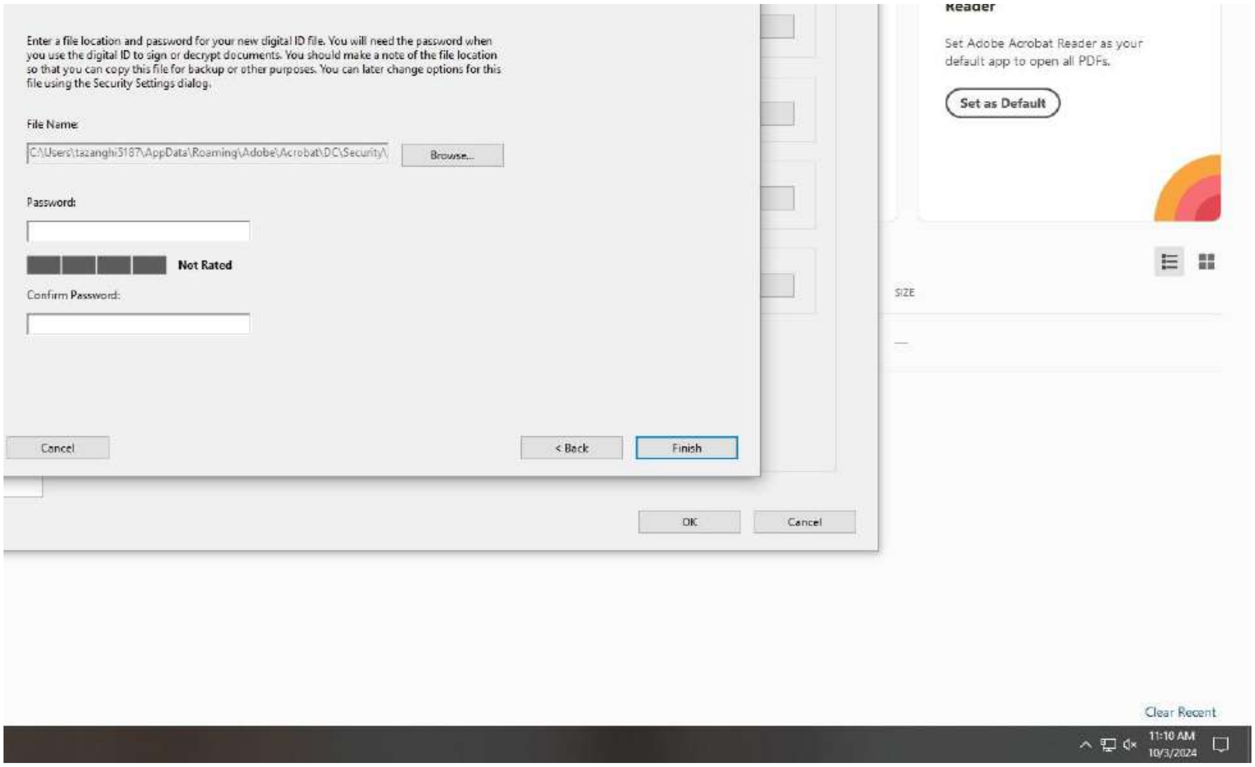
Country/Region: US - UNITED STATES

Key Algorithm: 2048-bit RSA

Use digital ID for: Digital Signatures and Data Encryption

Set Adobe Acrobat Reader as your default app to open all PDFs.

14. Enter the requested information. Under Key Algorithm, click the down arrow to display two options. The default is 2048-bit RSA, which provides more security, while 1024-bit RSA provides less security but is more universally compatible. Accept the 2048-bit RSA.



Enter a file location and password for your new digital ID file. You will need the password when you use the digital ID to sign or decrypt documents. You should make a note of the file location so that you can copy this file for backup or other purposes. You can later change options for this file using the Security Settings dialog.

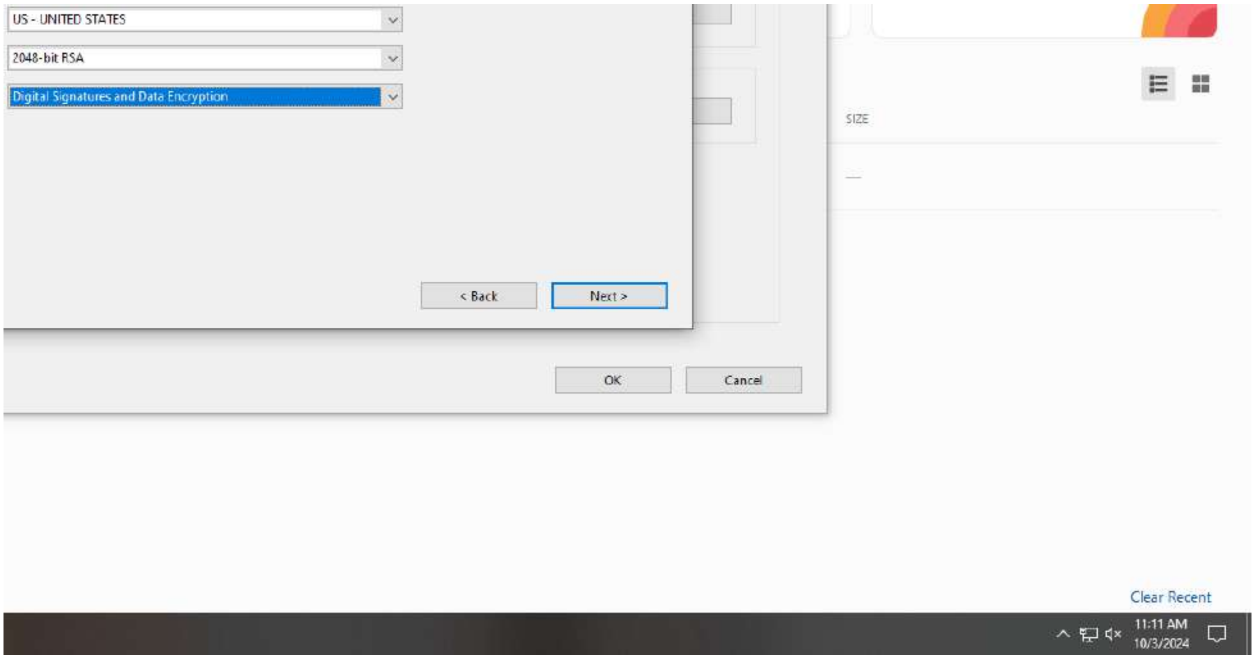
File Name: C:\Users\tazanghi5187\AppData\Roaming\Adobe\Acrobat\DC\Security\

Password:

Not Rated

Confirm Password:

15. Under Use digital ID for, click the down arrow to display three options. Select the default Digital Signatures and Data Encryption. Click Next.

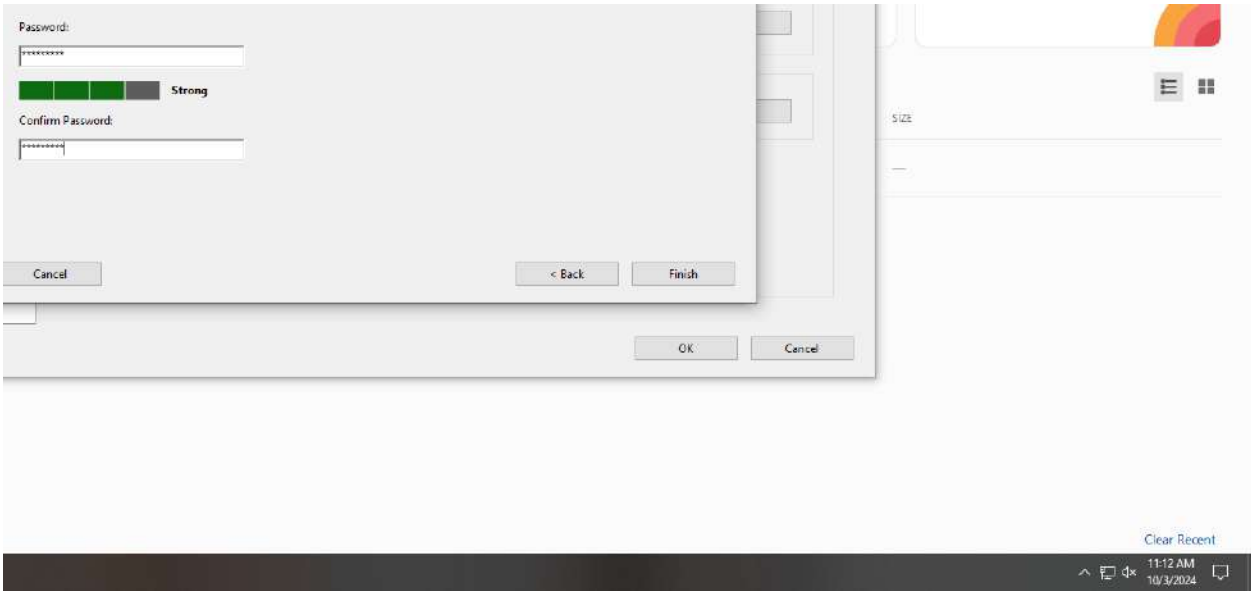


US - UNITED STATES

2048-bit RSA

Digital Signatures and Data Encryption

16. Create and enter a strong password, and then confirm that password. Click Finish.

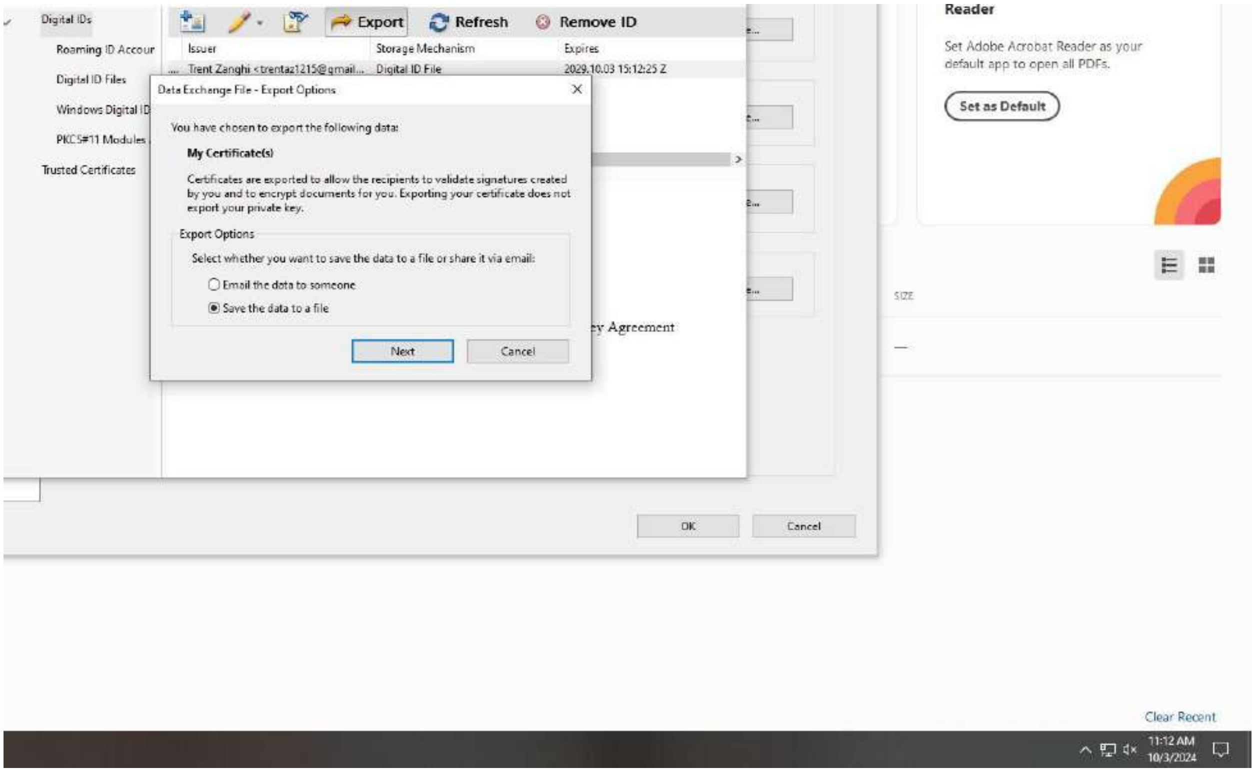


Password: *********

Strong

Confirm Password: *********

17. Your file is now created. Click Export.



Issuer	Storage Mechanism	Expires
Trent Zanghi <trentaz1215@gmail...	Digital ID File	2029.10.03 15:12:25 Z

Data Exchange File - Export Options

You have chosen to export the following data:

My Certificate(s)

Certificates are exported to allow the recipients to validate signatures created by you and to encrypt documents for you. Exporting your certificate does not export your private key.

Export Options

Select whether you want to save the data to a file or share it via email:

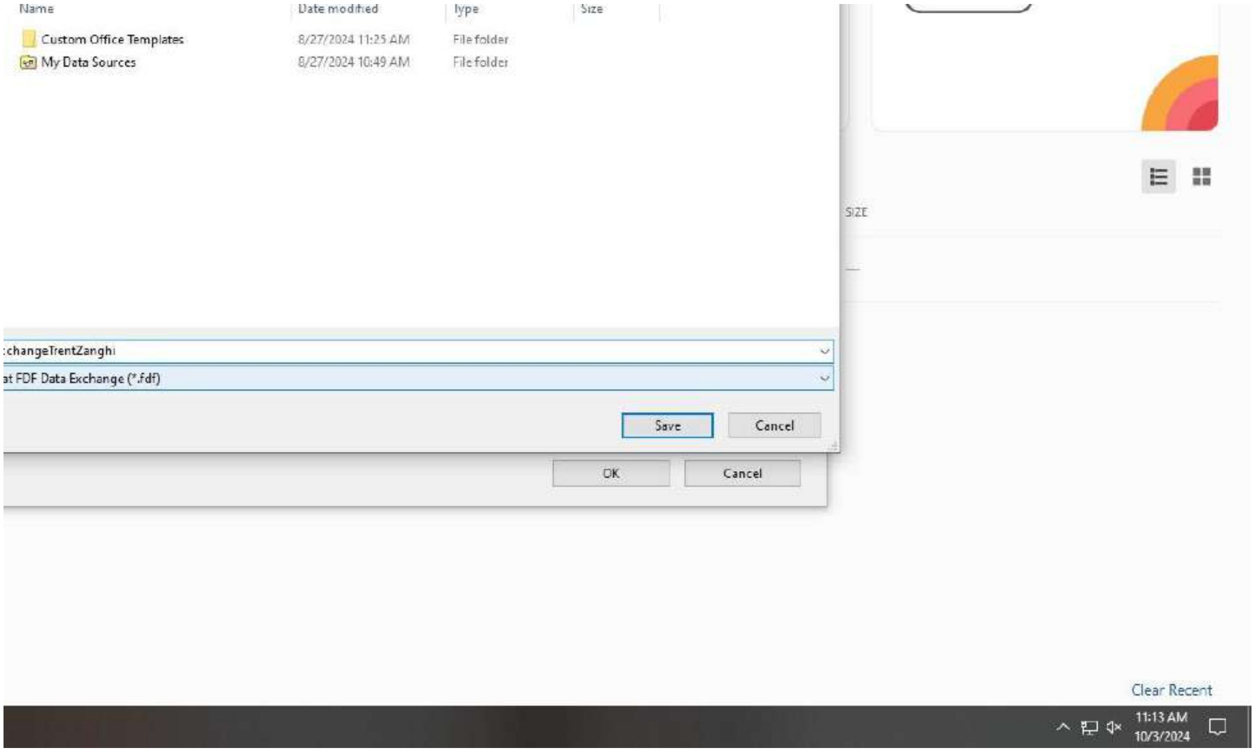
○ Email the data to someone

● Save the data to a file

Reader

Set Adobe Acrobat Reader as your default app to open all PDFs.

18. If necessary, click Save the data to a file and then click Next.

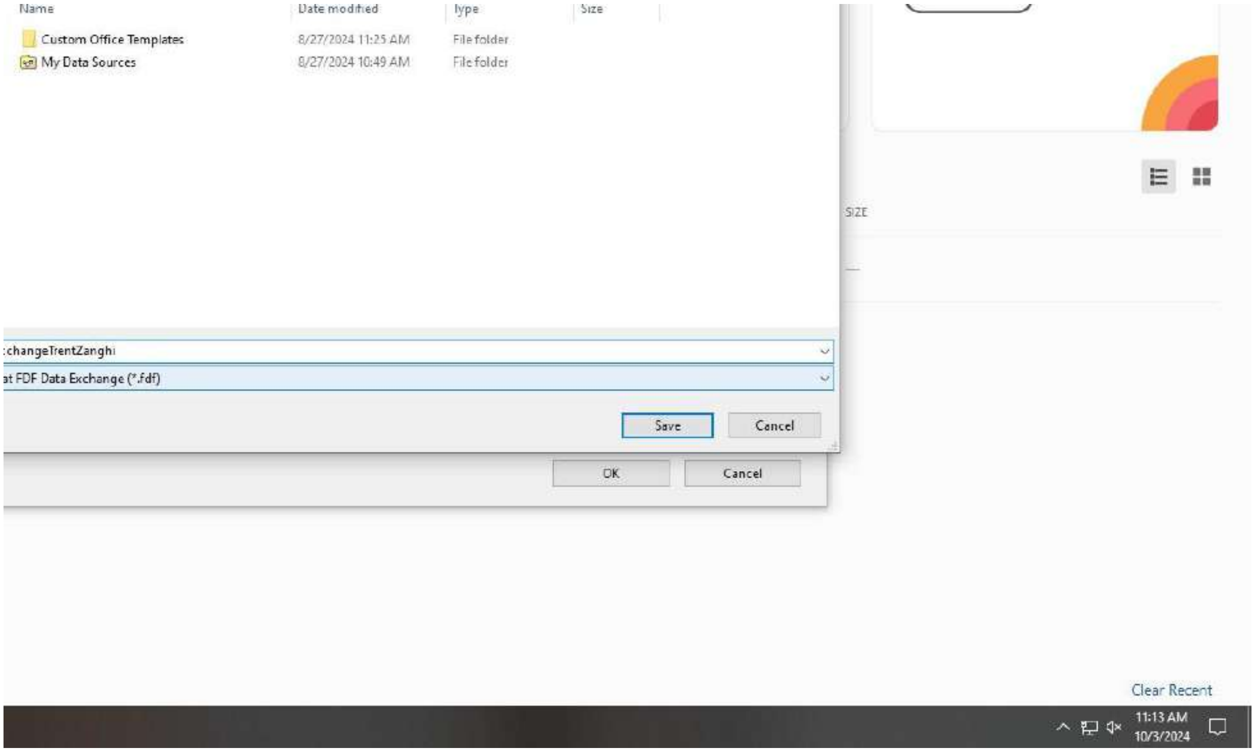


Name	Date modified	Type	Size
Custom Office Templates	8/27/2024 11:25 AM	File folder	
My Data Sources	8/27/2024 10:49 AM	File folder	

:changeTrentZanghi

at FDF Data Exchange (*.fdf)

19. Save the file to your computer.



Name	Date modified	Type	Size
Custom Office Templates	8/27/2024 11:25 AM	File folder	
My Data Sources	8/27/2024 10:49 AM	File folder	

:changeTrentZanghi

at FDF Data Exchange (*.fdf)

20. Close the windows associated with configuring your certificate. You can use this certificate by sending it to anyone who needs to validate your identity.

21. Close all windows.

Case Project 7-6: Digital Certificate Costs

Use the Internet to research the costs of the different types of digital certificates: domain validation, EV, wildcard, SAN, machine/computer, code signing, and email. Look up at least three providers of each, and create a table listing the type of certificate, the costs, and the length of time the certificate is valid.

Introduction:

When selecting a digital certificate, it's essential to understand the various types and their costs. Digital certificates vary in their scope, security level, and use cases, from basic Domain Validation (DV) to more complex Extended Validation (EV), Wildcard, SAN (Subject Alternative Name), machine/computer, code signing, and email certificates. Prices fluctuate depending on the provider, the type of certificate, and the level of validation required.

Certificate Type	Provider	Cost (Approx.)	Validity Period
Domain Validation	Comodo	$100/year	1 to 6 years
	DigiCert	$312-1296/year	1 year
	GeoTrust	$168/year	1 year
Extended Validation (EV)	Comodo	$99 - $1,200/year	1 to 2 years
	DigiCert	$468 - $1,860/year	1 to 2 years
	GlobalSign	$599/year	1 year
Wildcard	Comodo	$53 - $103/year	1 year
	DigiCert	$855 year	1 year
	GlobalSign	$849y ear	1 year
Subject Alternative Name (SAN)	Comodo	$227/year	1 year
	DigiCert	$1260/year	1 year
	GlobalSign	$849 /year	1 year
Machine/Computer	Comodo	$50 - $300/year	1 to 3 years
	DigiCert	$199 - $500/year	1 to 2 years

	GlobalSign	$300 - $600/year	1 to 2 years
Code Signing	Comodo	$219.45/year	1 year
	DigiCert	$588/year	1 year
	GlobalSign	$369/year	1 year
Email (S/MIME)	Comodo	$12/year	1 year
	DigiCert	$150/year	1 year
	GlobalSign	$39/year	1 year

References:

Cheap wildcard SSL certificate. Comodo. (2024). https://comodosslstore.com/promoads/wildcardssl.aspx?utm_source=bingCutm_medium=cpcCutm_campaign=Comodo+WildcardCutm_term=comodo+wildcardCmsclkid=8a6bceede6df1cfd1c9da9e0bd8fcef6

Digicert True Business ID. GeoTrust. (2024). https://www.geotrust.com/tls-ssl/tls-ssl-certificates

Digital Trust for the real world. DigiCert. (2024). https://www.digicert.com/#:~:text=%24100%20%2F%20month%20%2F%20standard,domain%2012%20month%20auto-renewing%20subscription%20%241%2C296.00

Wildcard SSL - SSL & Digital certificates by globalsign. GlobalSign. (2024). https://shop.globalsign.com/en/ssl/wildcard-ssl#:~:text=From%20%24849,USD%20%2Fyear

Assignment 4 – Hands On

Sam Peller

November 6, 2024

ISM 4323

project G-1: using glasswire Firewall

Time required: 25 minutes

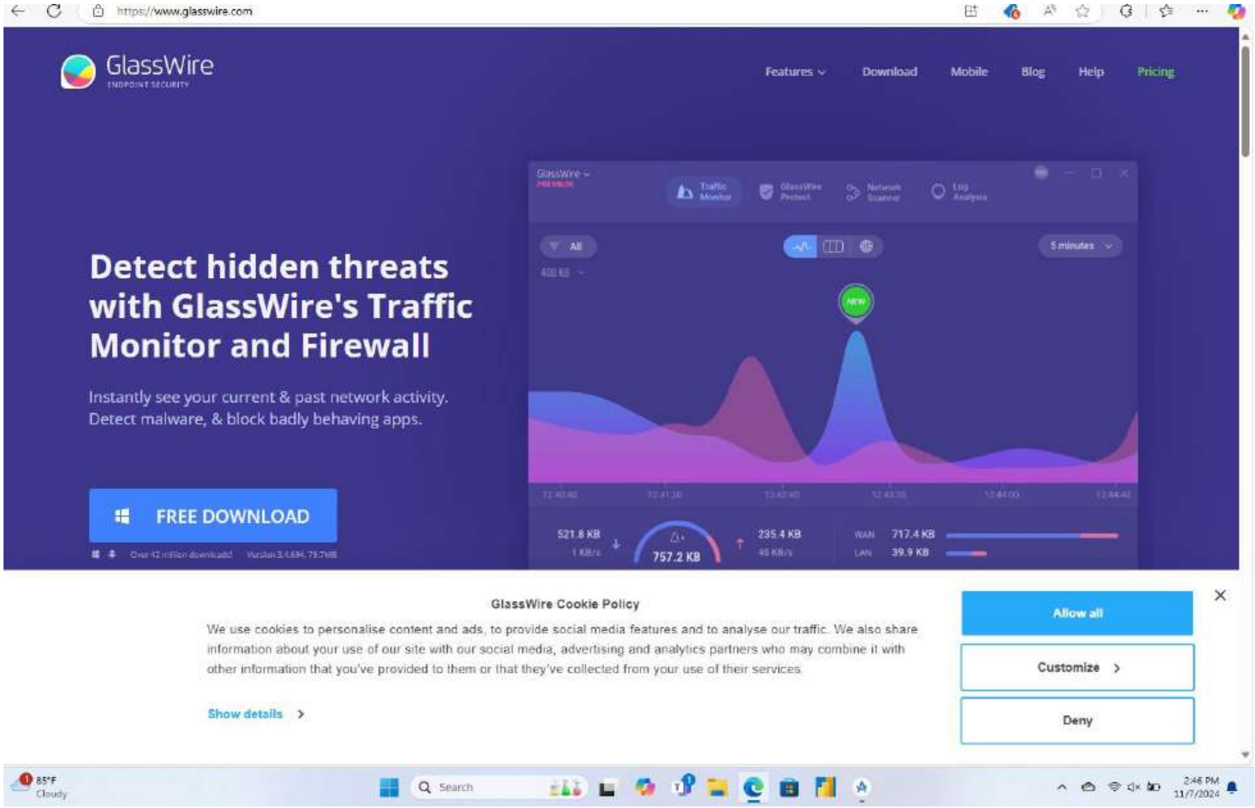
Objective: Given a scenario, implement secure network designs.

Description: GlassWire is a firewall and Security and Information Event Management (SIEM) product. In this activity, you will download and install GlassWire.

Introduction:

In today's digital landscape, securing network infrastructure is vital to protect against a wide array of cyber threats. With the rapid increase in sophisticated attacks, IT professionals are continuously exploring advanced tools and techniques to design and implement secure networks. One powerful approach involves using firewalls alongside Security and Information Event Management (SIEM) systems, which together provide real- time monitoring, analysis, and response capabilities to enhance network security. This activity focuses on GlassWire, which is a unique product that combines firewall capabilities with SIEM functionalities. GlassWire not only monitors network traffic but also provides alerts on potential security events, allowing users to manage and respond to threats proactively. its an invaluable asset in implementing secure network designs. This exercise highlights how firewalls and SIEM products can work together to maintain network integrity and protect sensitive data across diverse environments.

1. Use your web browser to go to www.glasswire.com. (If you are no longer able to access
the site through the URL, use a search engine to search for "GlassWire.")



Detect hidden threats with GlassWire's Traffic Monitor and Firewall

Instantly see your current & past network activity. Detect malware, & block badly behaving apps.

GlassWire Cookie Policy

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

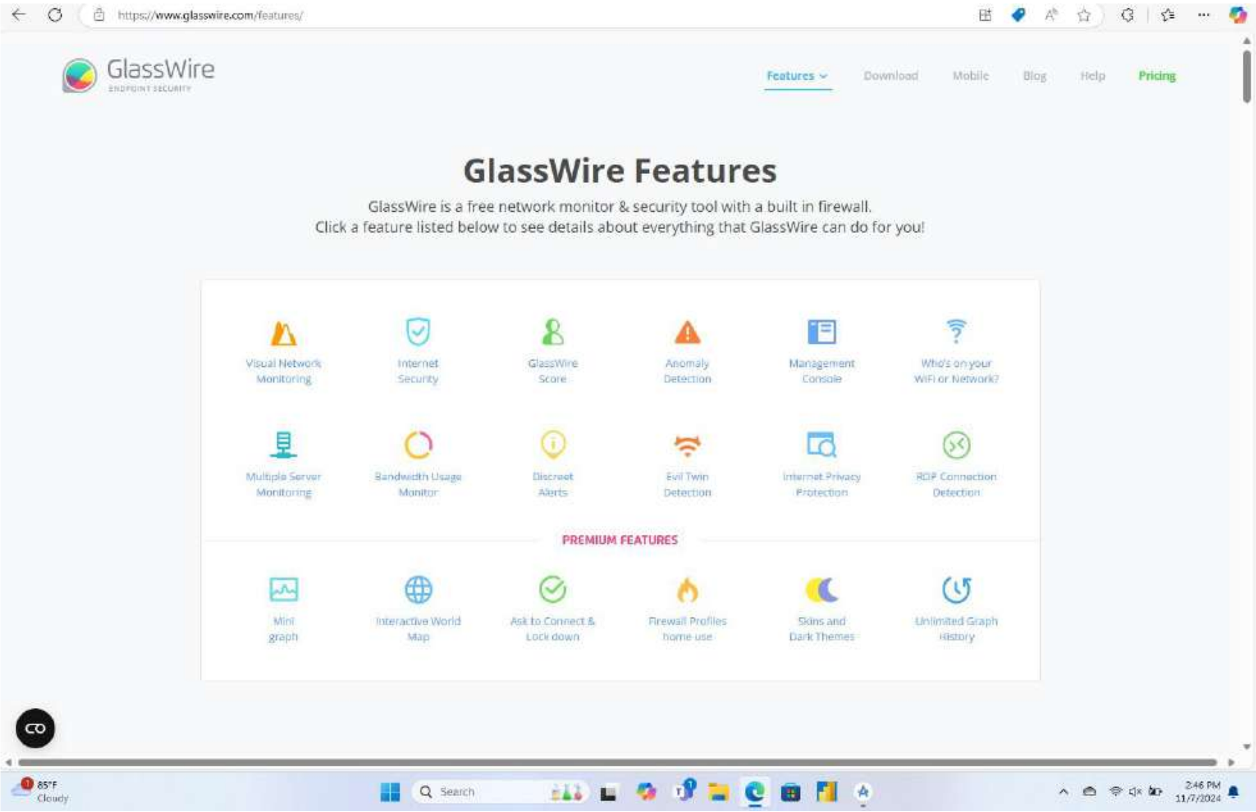
Show details >

Allow all

Customize >

Deny

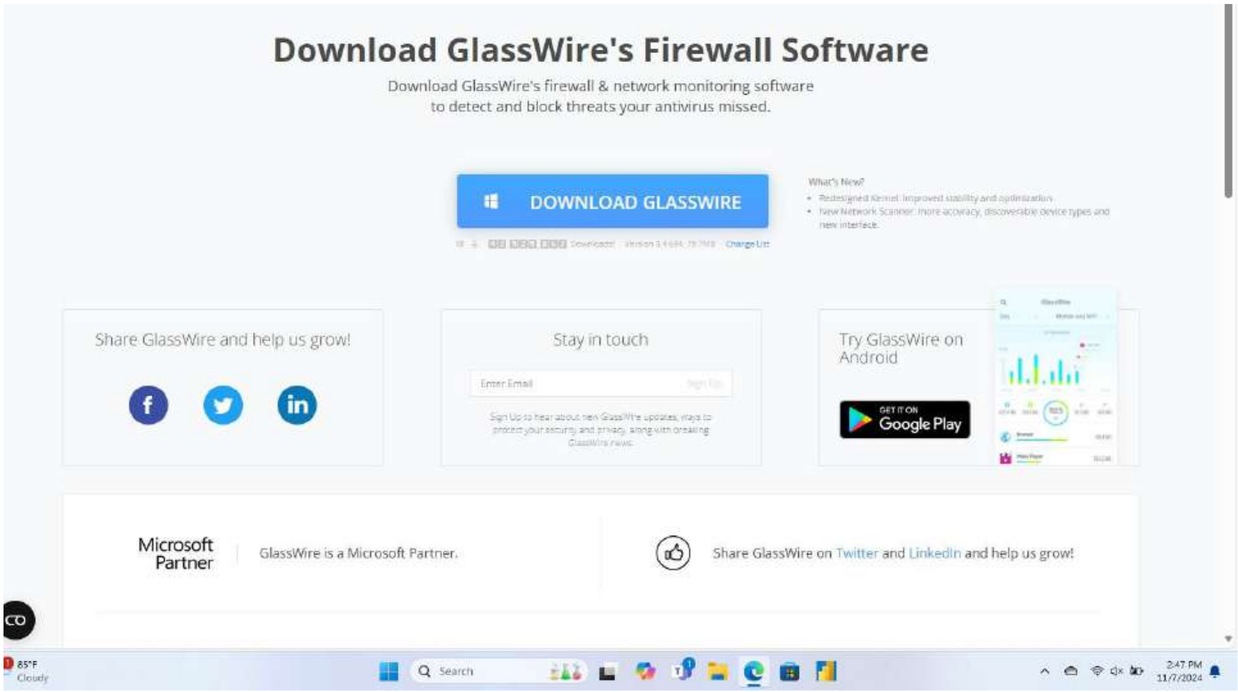
2. Click Features and scroll through the page to read about the different features and configuration options in this product.



GlassWire Features

GlassWire is a free network monitor & security tool with a built in firewall.
Click a feature listed below to see details about everything that GlassWire can do for you!

3. Click Free download and then click download Glass wire to download the file.



Download GlassWire's Firewall Software

Download GlassWire's firewall & network monitoring software
to detect and block threats your antivirus missed.

What's New?

- Redesigned Kernel: Improved stability and optimization.
- New Network Scanner: more accuracy, discoverable device types and new interface.

Share GlassWire and help us grow!

Stay in touch

Enter Email

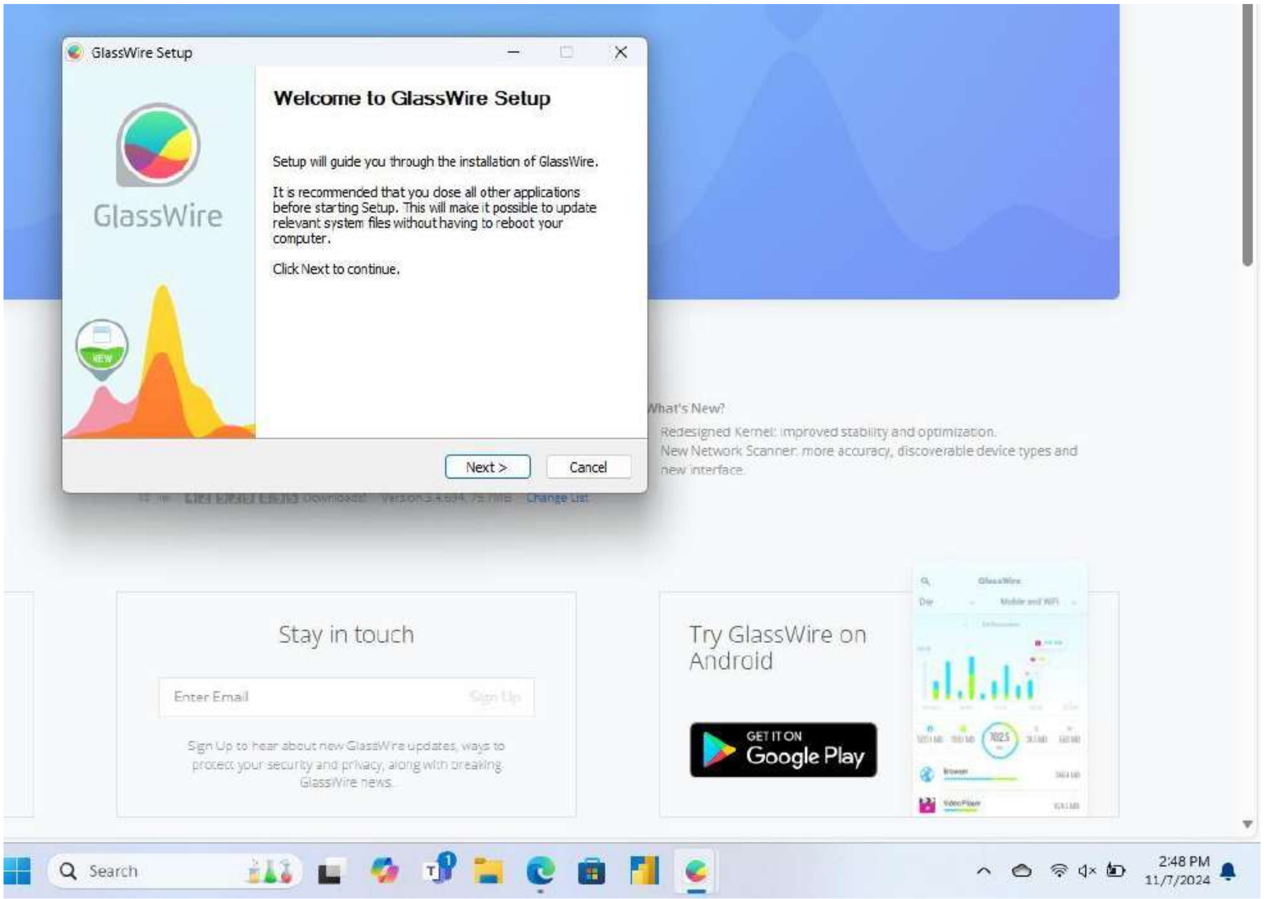
Sign Up to hear about new GlassWire updates, ways to protect your security and privacy, along with breaking GlassWire news.

Try GlassWire on Android

GlassWire is a Microsoft Partner.

Share GlassWire on Twitter and LinkedIn and help us grow!

4. Navigate to the location of the downloaded file GlasswireSetup.exe and launch this program to install GlassWire by accepting the default settings.



Welcome to GlassWire Setup

Setup will guide you through the installation of GlassWire.

It is recommended that you dose all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

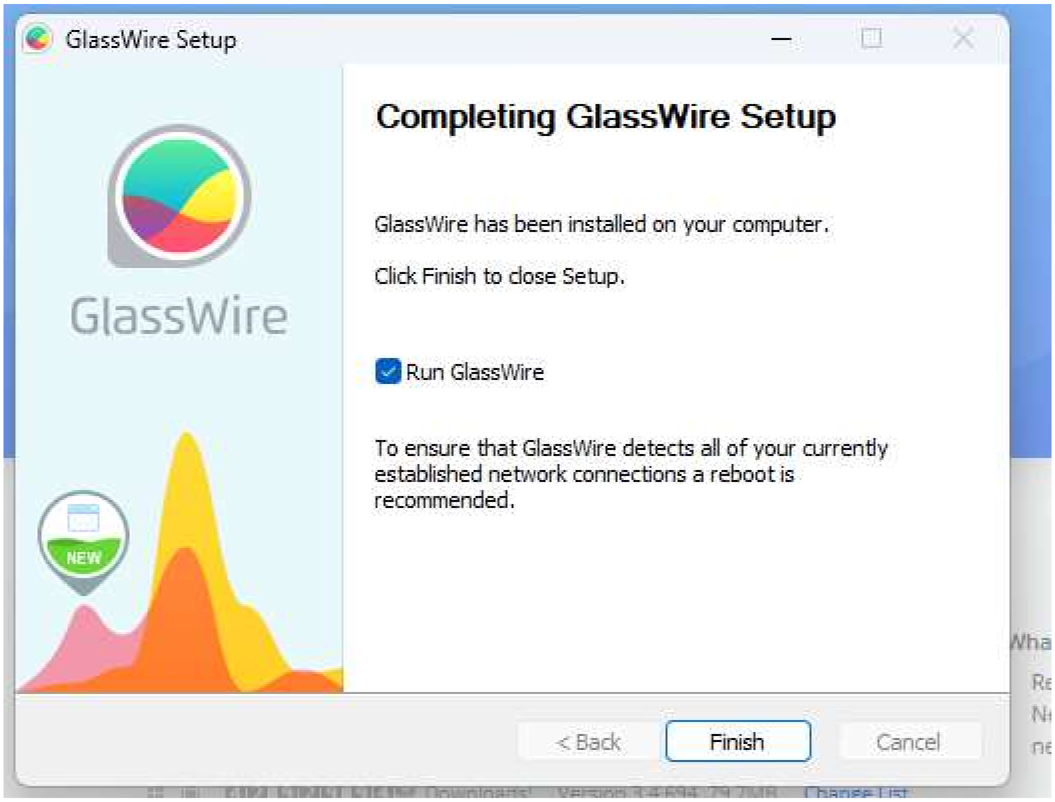
What's New?

Redesigned Kernel: improved stability and optimization.

New Network Scanner: more accuracy, discoverable device types and new interface.

Sign Up to hear about new GlassWire updates, ways to protect your security and privacy, along with breaking GlassWire news.

5. Click Finish to run GlassWire.



Completing GlassWire Setup

GlassWire has been installed on your computer.

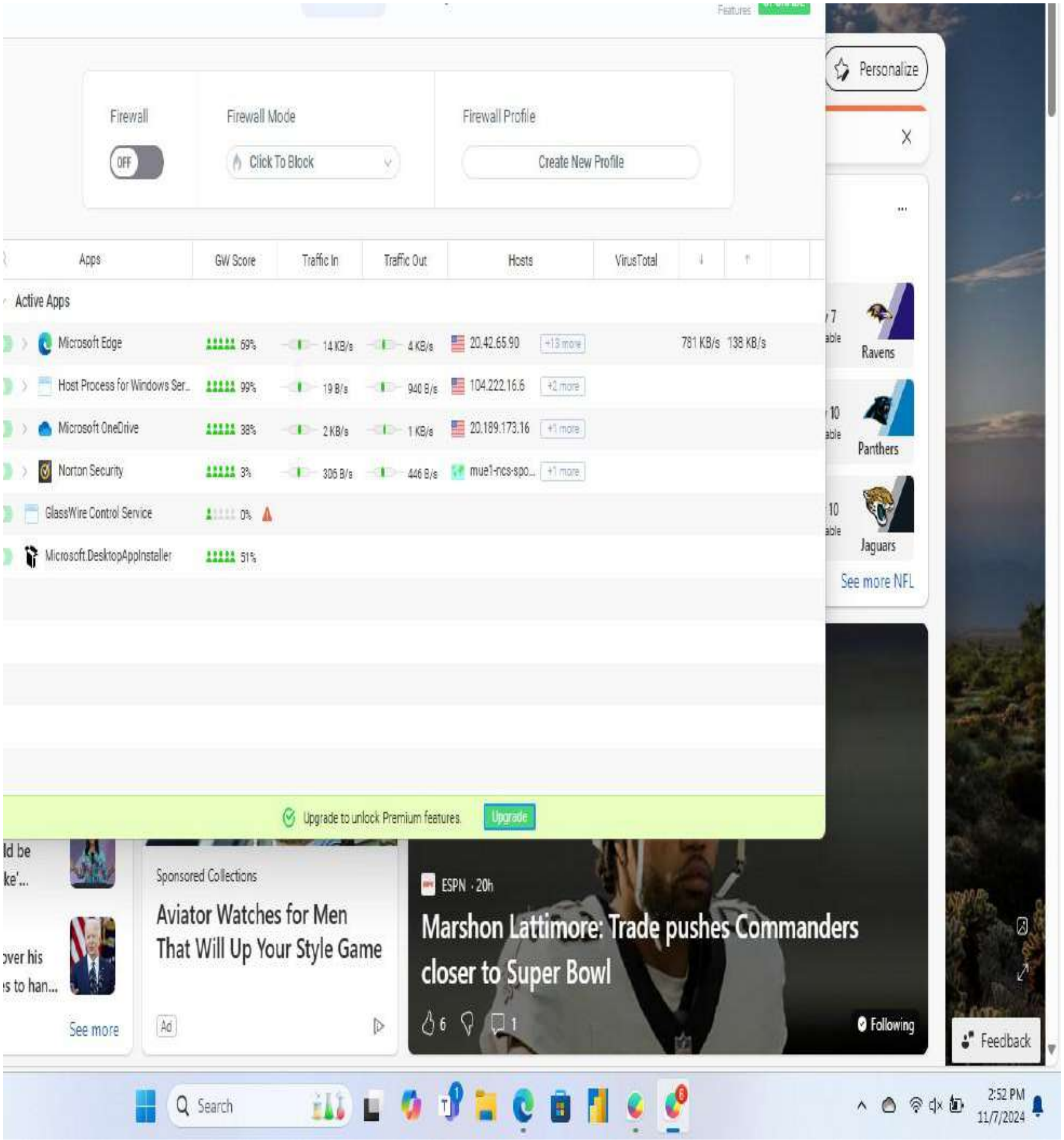
Click Finish to close Setup.

☑ Run GlassWire

To ensure that GlassWire detects all of your currently established network connections a reboot is recommended.

6. Note that the information scrolls horizontally to the left regarding events that are occurring. Open a web browser and surf the Internet for several minutes.

7. Return to GlassWire.



Firewall: OFF

Firewall Mode: Click To Block

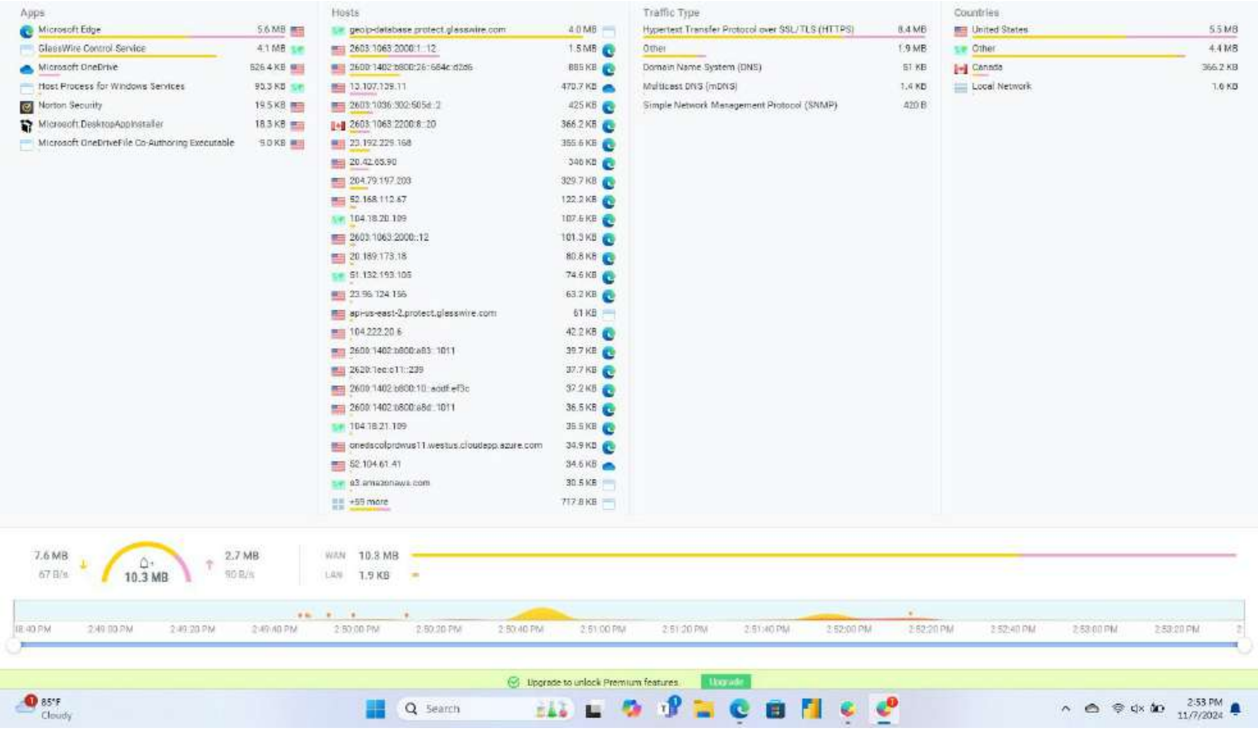
Firewall Profile: Create New Profile

Apps	GW Score	Traffic In	Traffic Out	Hosts	VirusTotal	↓	↑
Active Apps							
Microsoft Edge	69%	14 KB/s	4 KB/s	20.42.65.90 +13 more		781 KB/s	138 KB/s
Host Process for Windows Ser...	99%	19 B/s	940 B/s	104.222.16.6 +2 more			
Microsoft OneDrive	38%	2 KB/s	1 KB/s	20.189.173.16 +1 more			
Norton Security	3%	306 B/s	446 B/s	mue1-ncs-spo... +1 more			
GlassWire Control Service	0% ⚠						
Microsoft.DesktopAppInstaller	51%						

Upgrade to unlock Premium features. Upgrade

8. Slide the scroller at the bottom of the screen to consolidate the views.

9. Click Apps. What information is given in the left pane? How can this be useful?



Apps	
Microsoft Edge	5.6 MB
GlassWire Control Service	4.1 MB
Microsoft OneDrive	526.4 KB
Host Process for Windows Services	95.3 KB
Norton Security	19.5 KB
Microsoft.DesktopAppInstaller	18.3 KB
Microsoft OneDriveFile Co-Authoring Executable	9.0 KB

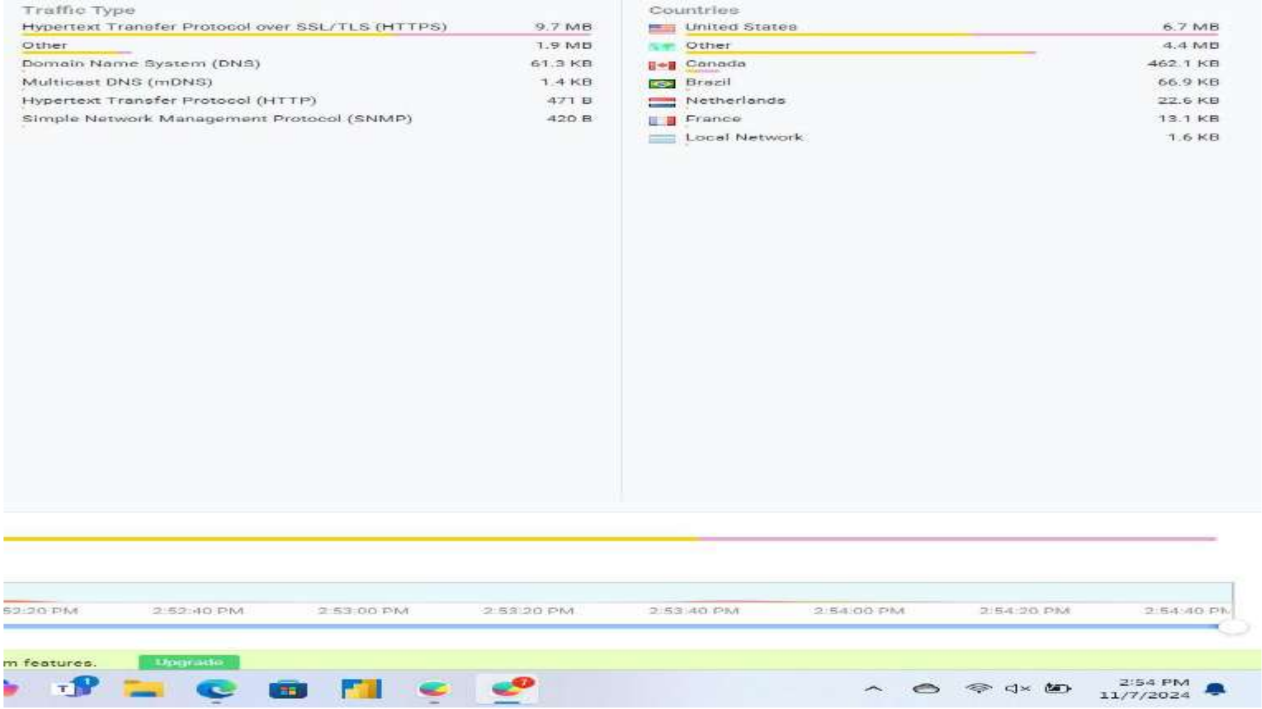
Hosts	
geoip-database.protect.glasswire.com	4.0 MB
2603:1063:2000:1::12	1.5 MB
2600:1402:b800:26::684c:d2d6	885 KB
13.107.139.11	470.7 KB
2603:1036:302:505d::2	425 KB
2603:1063:2200:8::20	366.2 KB
23.192.229.168	355.6 KB
20.42.65.90	346 KB
204.79.197.203	329.7 KB
52.168.112.67	122.2 KB
104.18.20.109	107.6 KB
2603:1063:2000::12	101.3 KB
20.189.173.18	80.8 KB
51.132.193.105	74.6 KB
23.96.124.156	63.2 KB
api-us-east-2.protect.glasswire.com	61 KB
104.222.20.6	42.2 KB
2600:1402:b800:a83::1011	39.7 KB
2620:1ec:c11::239	37.7 KB
2600:1402:b800:10::aodf:ef3c	37.2 KB
2600:1402:b800:a8d::1011	36.5 KB
104.18.21.109	35.5 KB
onedscolprdwus11.westus.cloudapp.azure.com	34.9 KB
52.104.61.41	34.6 KB
s3.amazonaws.com	30.5 KB
+59 more	717.8 KB

Traffic Type	
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	8.4 MB
Other	1.9 MB
Domain Name System (DNS)	61 KB
Multicast DNS (mDNS)	1.4 KB
Simple Network Management Protocol (SNMP)	420 B

Countries	
United States	5.5 MB
Other	4.4 MB
Canada	366.2 KB
Local Network	1.6 KB

It can highlight the consumption of each app

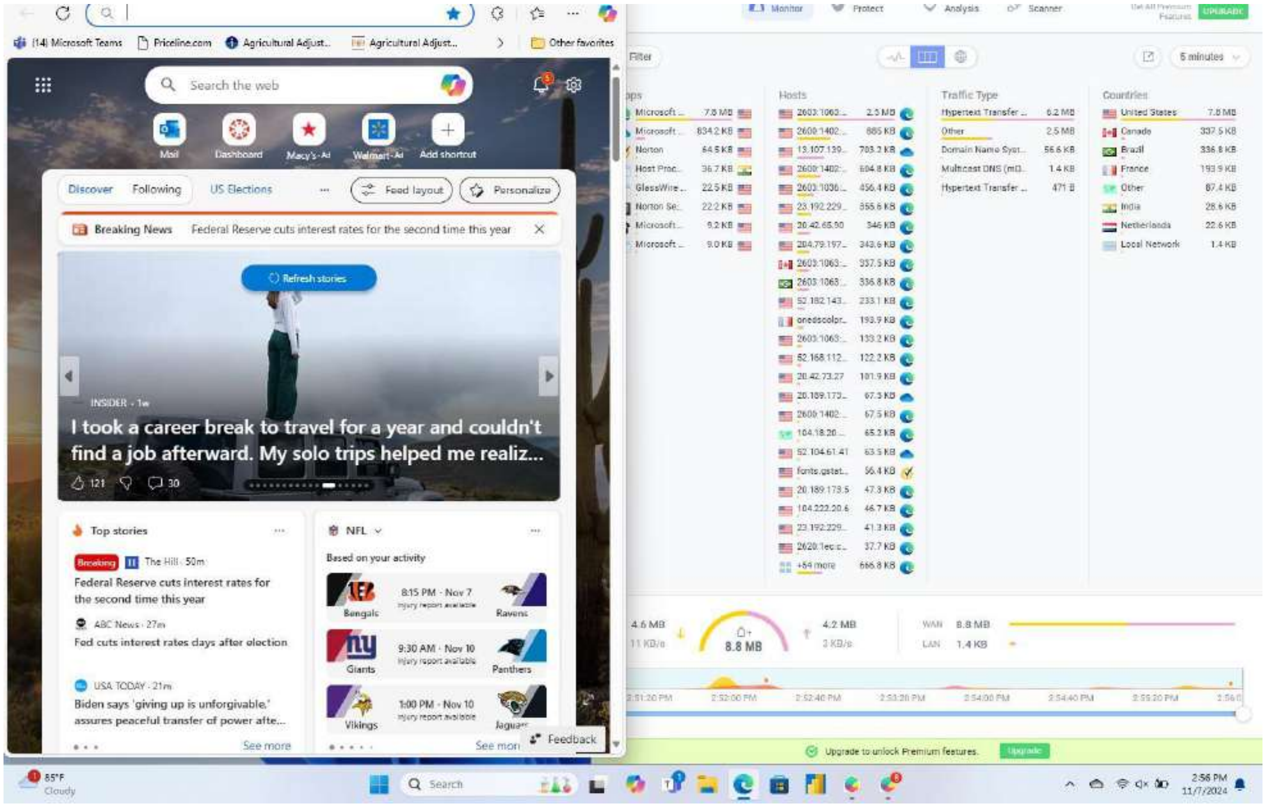
10. Click Traffic to view an analysis of the different traffic types.



Traffic Type	
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	9.7 MB
Other	1.9 MB
Domain Name System (DNS)	61.3 KB
Multicast DNS (mDNS)	1.4 KB
Hypertext Transfer Protocol (HTTP)	471 B
Simple Network Management Protocol (SNMP)	420 B

Countries	
United States	6.7 MB
Other	4.4 MB
Canada	462.1 KB
Brazil	66.9 KB
Netherlands	22.6 KB
France	13.1 KB
Local Network	1.6 KB

11. Open a web browser, and then arrange the GlassWire window and the browser window side by side on your computer screen.



Breaking News Federal Reserve cuts interest rates for the second time this year

INSIDER · 1w
I took a career break to travel for a year and couldn't find a job afterward. My solo trips helped me realiz...
121 30

Breaking The Hill · 50m
Federal Reserve cuts interest rates for the second time this year

ABC News · 27m
Fed cuts interest rates days after election

USA TODAY · 21m
Biden says 'giving up is unforgivable,' assures peaceful transfer of power afte...

Based on your activity

Bengals	8:15 PM · Nov 7 Injury report available	Ravens
Giants	9:30 AM · Nov 10 Injury report available	Panthers
Vikings	1:00 PM · Nov 10 Injury report available	Jaguars

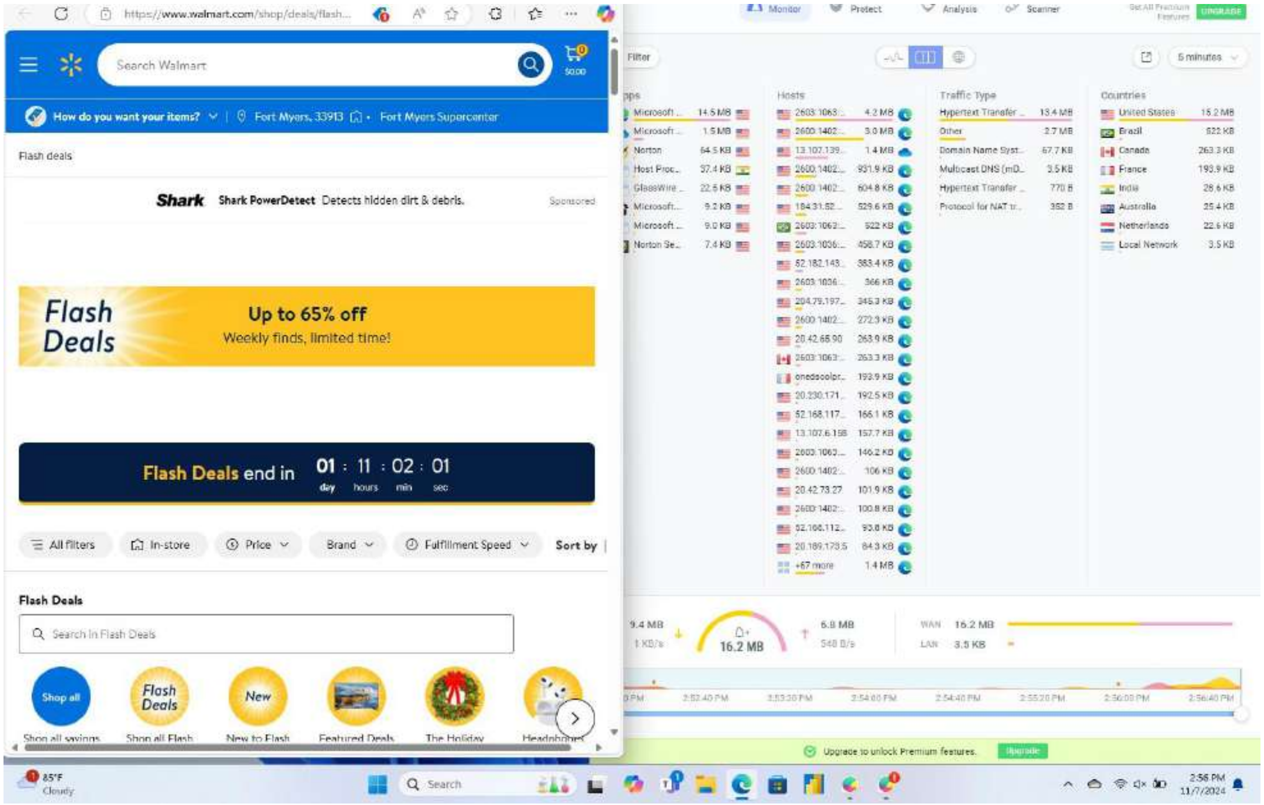
Apps	
Microsoft ...	7.8 MB
Microsoft ...	834.2 KB
Norton	64.5 KB
Host Proc...	36.7 KB
GlassWire ...	22.5 KB
Norton Se...	22.2 KB
Microsoft...	9.2 KB
Microsoft ...	9.0 KB

Hosts	
2603:1063:...	2.5 MB
2600:1402:...	885 KB
13.107.139...	703.2 KB
2600:1402:...	604.8 KB
2603:1036:...	456.4 KB
23.192.229...	355.6 KB
20.42.65.90	346 KB
204.79.197...	343.6 KB
2603:1063:...	337.5 KB
2603:1063:...	336.8 KB
52.182.143...	233.1 KB
onedscolpr...	193.9 KB
2603:1063:...	133.2 KB
52.168.112...	122.2 KB
20.42.73.27	101.9 KB
20.189.173...	67.3 KB
2600:1402:...	67.5 KB
104.18.20....	65.2 KB
52.104.61.41	63.5 KB
fonts.gstat...	56.4 KB
20.189.173.5	47.3 KB
104.222.20.6	46.7 KB
23.192.229...	41.3 KB
2620:1ec:c...	37.7 KB
+54 more	666.8 KB

Traffic Type	
Hypertext Transfer ...	6.2 MB
Other	2.5 MB
Domain Name Syst...	56.6 KB
Multicast DNS (mD...	1.4 KB
Hypertext Transfer ...	471 B

Countries	
United States	7.8 MB
Canada	337.5 KB
Brazil	336.8 KB
France	193.9 KB
Other	87.4 KB
India	28.6 KB
Netherlands	22.6 KB
Local Network	1.4 KB

12. Use your web browser to surf the web, and watch the GlassWire screen as well. What can you learn from this?



Apps	
Microsoft ...	14.5 MB
Microsoft ...	1.5 MB
Norton	64.5 KB
Host Proc...	37.4 KB
GlassWire ...	22.6 KB
Microsoft...	9.2 KB
Microsoft ...	9.0 KB
Norton Se...	7.4 KB

Hosts	
2603:1063:...	4.2 MB
2600:1402:...	3.0 MB
13.107.139...	1.4 MB
2600:1402:...	931.9 KB
2600:1402:...	604.8 KB
184.31.52...	529.6 KB
2603:1063:...	522 KB
2603:1036:...	458.7 KB
52.182.143...	383.4 KB
2603:1036:...	366 KB
204.79.197...	345.3 KB
2600:1402:...	272.3 KB
20.42.65.90	263.9 KB
2603:1063:...	263.3 KB
onedscolpr...	193.9 KB
20.230.171...	192.5 KB
52.168.117...	166.1 KB
13.107.6.158	157.7 KB
2603:1063:...	146.2 KB
2600:1402:...	106 KB
20.42.73.27	101.9 KB
2600:1402:...	100.8 KB
52.168.112...	93.8 KB
20.189.173.5	84.3 KB
+67 more	1.4 MB

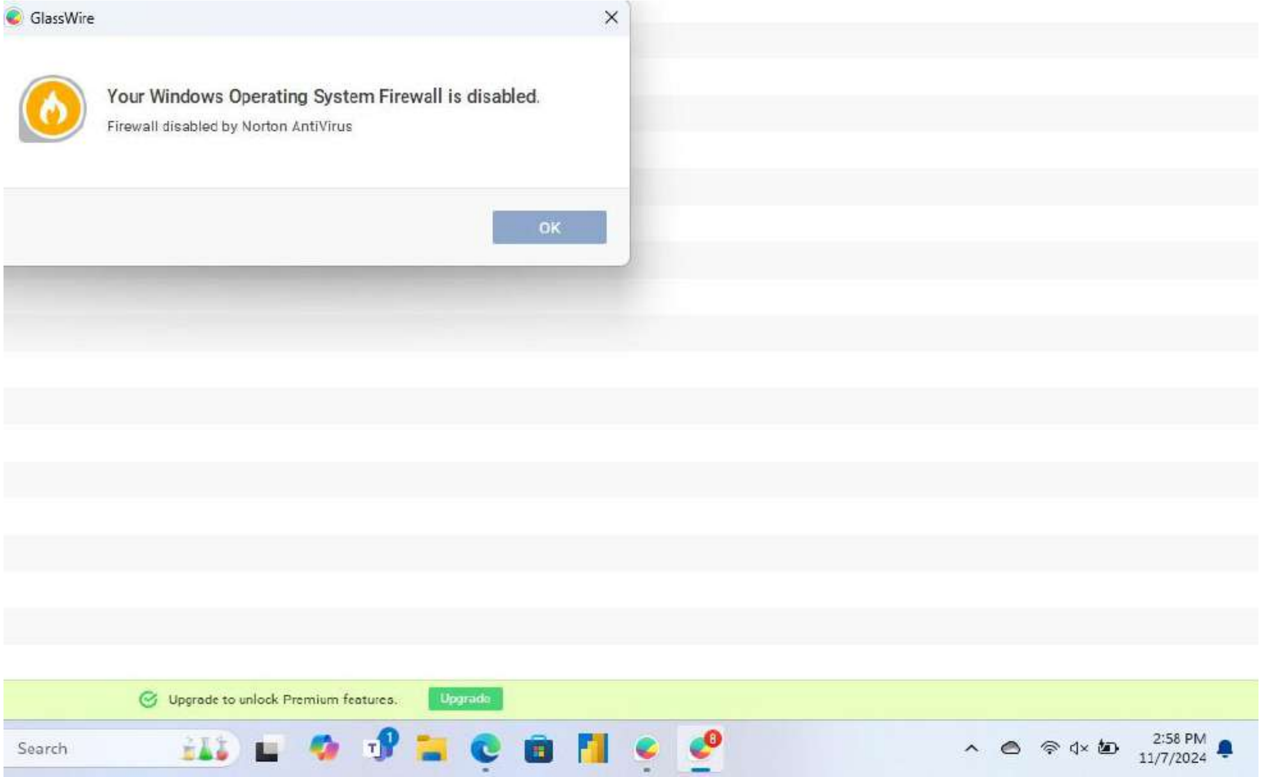
Traffic Type	
Hypertext Transfer ...	13.4 MB
Other	2.7 MB
Domain Name Syst...	67.7 KB
Multicast DNS (mD...	3.5 KB
Hypertext Transfer ...	770 B
Protocol for NAT tr...	352 B

Countries	
United States	15.2 MB
Brazil	522 KB
Canada	263.3 KB
France	193.9 KB
India	28.6 KB
Australia	25.4 KB
Netherlands	22.6 KB
Local Network	3.5 KB

It will update in real time to show new hosts and their countries

13. Close the browser window and maximize GlassWire.

14. Click the Firewall button. What apps or services have recently gone through your firewall?



GlassWire

Your Windows Operating System Firewall is disabled.

Firewall disabled by Norton AntiVirus

N/A

15. Click the usage button to see a summary of the local Apps utilized, the Hosts accessed, and the Traffic Type.

16. Click Alerts. Scroll through any alerts that have been issued. What can you tell about them?

The outputs vary

17. How valuable is this information from GlassWire?

For me it is only slightly valuable because I don't know what to do with some of the information. For a professional it could be very valuable depending on the goal.

18. Close all windows.

case project G-5: UTM comparison

Description: Create a table of four UTM devices available today. Include the vendor's name, pricing, a list of features, the type of protections it provides, etc. Based on your research, assign a value of 1–5 (from lowest to highest ranking) that you would give that UTM. Include a short explanation of why you gave it that ranking

Introduction:

Unified Threat Management (UTM) devices are integral to modern network security, providing a comprehensive solution that combines multiple security functions within a single platform. UTMs typically offer features such as firewalls, intrusion prevention systems, antivirus protection, and web filtering, helping organizations streamline their security infrastructure and simplify network management. With cyber threats evolving, selecting a reliable UTM device that meets organizational needs and budget constraints is crucial for maintaining robust network defenses.

Vendor	Model	Pricing	Features	Protections Provided	Rating	Explanation
Cisco	Firepower NGFW	Starting at $595	IPS, Advanced Malware Protection (AMP), URL Filtering, VPN, Application Control	Network, Web, Application, Intrusion Prevention	5	Cisco's Firepower NGFW offers advanced security features suitable for various business sizes. Integration with Defense Orchestrator simplifies management, though its high cost may limit smaller enterprises.
Fortine t	FortiGate NGFW	Starts at $499	SD-WAN, Zero Trust Network Access, AI Threat Detection,	Network, Malware, Web, Threat Intelligence	4	FortiGate's AI-driven threat detection and comprehensive UTM suite make it a powerful option for

			Intrusion Prevention, Sandboxing			enterprises with high traffic volumes, though it has a learning curve.
Sopho s	UTM	Approx. $350/year	Advanced Threat Protection (ATP), Intrusion Prevention System (IPS), VPN, Email/Web Filtering	Network, Email, Web, Application	4	Sophos UTM's modular, intuitive design is ideal for mid-sized and smaller businesses. However, it lacks some cloud integration capabilities seen in more advanced systems.
Watch Guard	Firebo x	Starting at $520	Gateway Antivirus, URL Filtering, VPN, Application Layer Inspection, Behavioral Sandbox Detection	Network, Malware, Web, Application	3	WatchGuard Firebox is cost-effective and well- suited to smaller businesses, though it lacks advanced threat intelligence integrations found in higher-end options.

Project 8-3: mac spoofing

Time required: 25 minutes

objective: Given a scenario, analyze potential indicators associated with network attacks.

description: In a Mac cloning attack, threat actors discover a valid Mac address of a device connected to a switch. They spoof the Mac address on their device and send a packet onto the network. In this activity, you will spoof a Mac address.

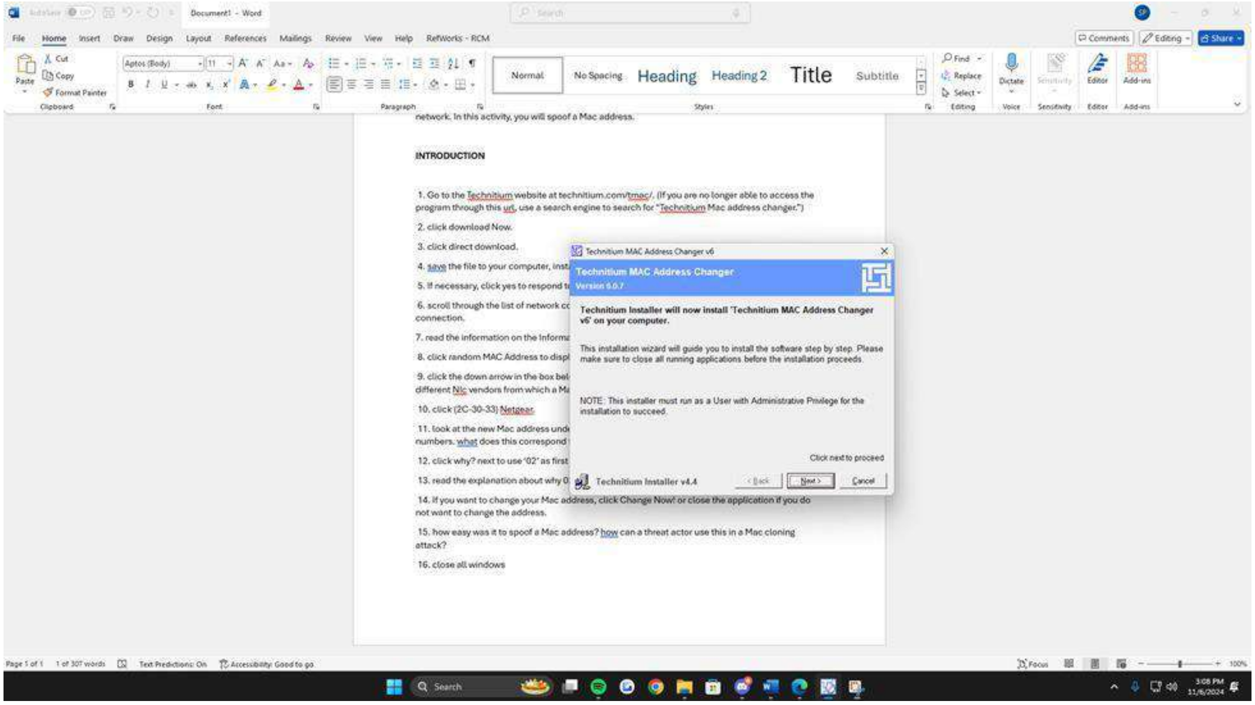
INTRODUCTION

A Media Access Control (MAC) address is a number assigned to network devices to identify individual devices. In a MAC cloning attack, attackers can exploit them for unauthorized access or disruption. By identifying the valid MAC addresses on a network, attackers can spoof this address on their own device and send malicious packets onto the network impersonating that device (Cranor, 2021). They can bypass MAC filtering security measures utilizing this spoof and this lab will demonstrate how easy it is to change your own MAC address.

1. Go to the Technitium website at technitium.com/tmac/. (If you are no longer able to access the
program through this url, use a search engine to search for “Technitium Mac address changer.”)

2. click download Now.

3. click direct download.



network. In this activity, you will spoof a Mac address.

INTRODUCTION

1. Go to the Technitium website at technitium.com/tmac/. (If you are no longer able to access the program through this url, use a search engine to search for "Technitium Mac address changer.")

2. click download Now.

3. click direct download.

4. save the file to your computer, inst

5. If necessary, click yes to respond t

6. scroll through the list of network co connection.

7. read the information on the Informa

8. click random MAC Address to displ

9. click the down arrow in the box bel different Nic vendors from which a M

10. click (2C-30-33) Netgear.

11. look at the new Mac address unde numbers. what does this correspond

12. click why? next to use '02' as first

13. read the explanation about why 0

14. If you want to change your Mac address, click Change Now! or close the application if you do not want to change the address.

15. how easy was it to spoof a Mac address? how can a threat actor use this in a Mac cloning attack?

16. close all windows

Technitium MAC Address Changer v6

Technitium MAC Address Changer
Version 6.0.7

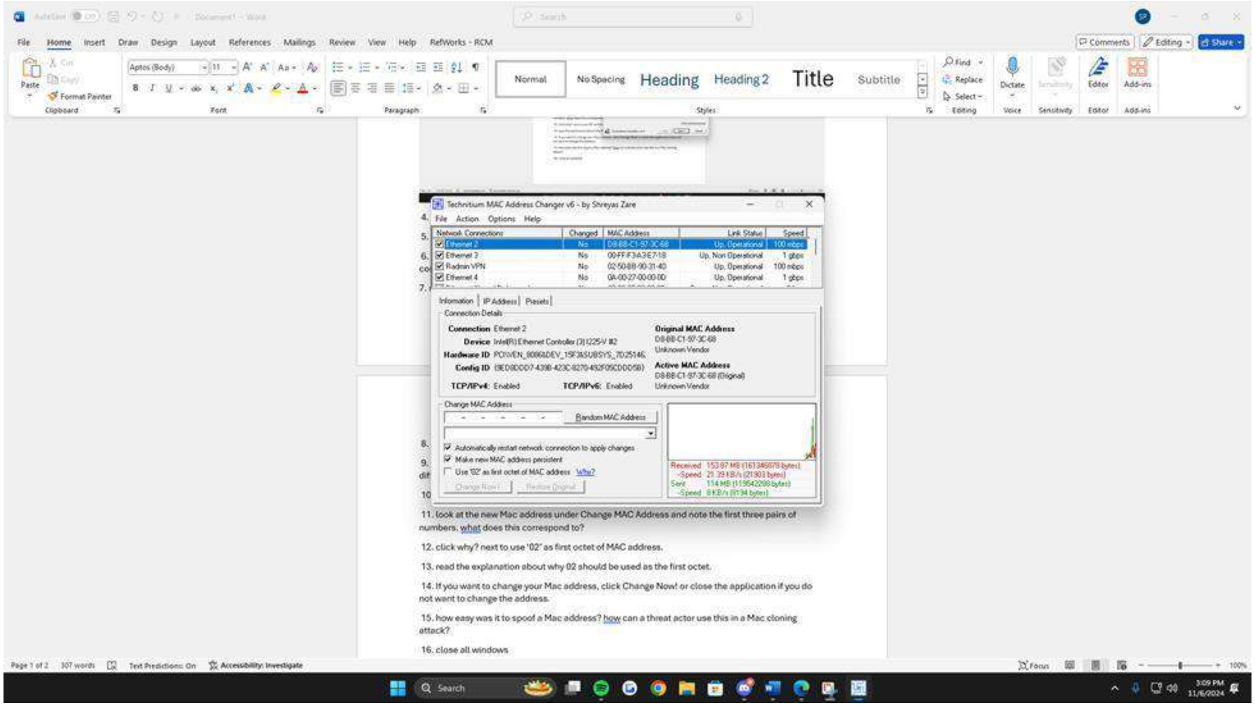
Technitium Installer will now install 'Technitium MAC Address Changer v6' on your computer.

This installation wizard will guide you to install the software step by step. Please make sure to close all running applications before the installation proceeds.

NOTE: This installer must run as a User with Administrative Privilege for the installation to succeed.

Click next to proceed

4. save the file to your computer, install the application, and then start it.



Technitium MAC Address Changer v6 - by Shreyas Zare

Network Connections	Changed	MAC Address	Link Status	Speed
☑ Ethernet 2	No	D8-BB-C1-97-3C-68	Up, Operational	100 mbps
☑ Ethernet 3	No	00-FF-F3-A3-E7-18	Up, Non Operational	1 gbps
☑ Radmin VPN	No	02-50-BB-90-31-40	Up, Operational	100 mbps
☑ Ethernet 4	No	0A-00-27-00-00-0D	Up, Operational	1 gbps

Connection Details

Connection: Ethernet 2
Device: Intel(R) Ethernet Controller (3) I225-V #2
Hardware ID: PCI\VEN_8086&DEV_15F3&SUBSYS_7D25146
Config ID: {9ED8DDD7-439B-423C-8270-492F05CDDD5B}
TCP/IPv4: Enabled TCP/IPv6: Enabled

Original MAC Address
D8-BB-C1-97-3C-68
Unknown Vendor

Active MAC Address
D8-BB-C1-97-3C-68 (Original)
Unknown Vendor

Change MAC Address

☑ Automatically restart network connection to apply changes
☑ Make new MAC address persistent
☐ Use '02' as first octet of MAC address Why?

Received 153.87 MB (161346878 bytes)
-Speed 21.39 KB/s (21903 bytes)
Sent 114 MB (119542288 bytes)
-Speed 8 KB/s (8194 bytes)

11. look at the new Mac address under Change MAC Address and note the first three pairs of numbers. what does this correspond to?

12. click why? next to use '02' as first octet of MAC address.

13. read the explanation about why 02 should be used as the first octet.

14. If you want to change your Mac address, click Change Now! or close the application if you do not want to change the address.

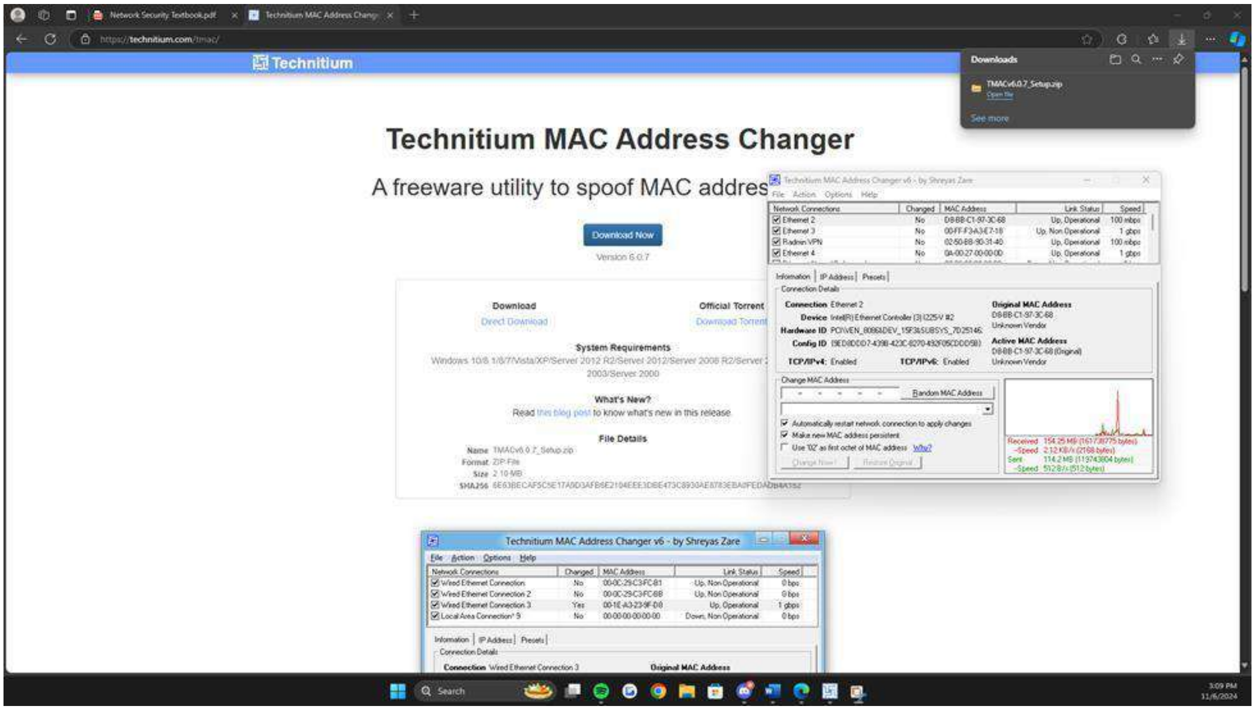
15. how easy was it to spoof a Mac address? how can a threat actor use this in a Mac cloning attack?

16. close all windows

5. If necessary, click yes to respond to the dialog box.

6. scroll through the list of network connections on your computer, and then select your Internet connection.

7. read the information on the Information tab.



https://technitium.com/tmac/

Technitium MAC Address Changer

A freeware utility to spoof MAC addres

Version 6.0.7

Download
Direct Download

Official Torrent
Download Torrent

System Requirements
Windows 10/8.1/8/7/Vista/XP/Server 2012 R2/Server 2012/Server 2008 R2/Server 2003/Server 2000

What's New?
Read this blog post to know what's new in this release

File Details
Name TMACv6.0.7_Setup.zip
Format ZIP File
Size 2.10 MB
SHA256 6E63BECAF5C5E17A9D3AFB6E2104EEE3DBE473C8930AE8783EBA0FEDADB4A152

Technitium MAC Address Changer v6 - by Shreyas Zare

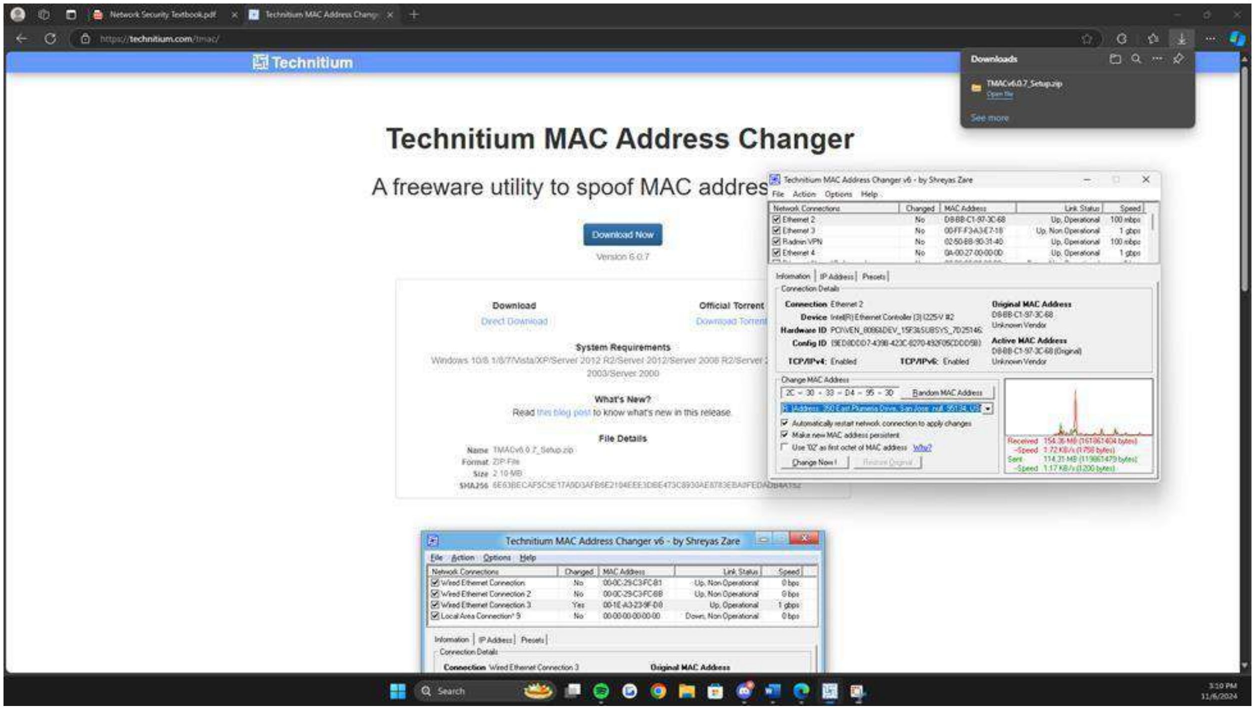
Network Connections	Changed	MAC Address	Link Status	Speed
☑ Wired Ethernet Connection	No	00-0C-29-C3-FC-B1	Up, Non Operational	0 bps
☑ Wired Ethernet Connection 2	No	00-0C-29-C3-FC-BB	Up, Non Operational	0 bps
☑ Wired Ethernet Connection 3	Yes	00-1E-A3-23-9F-D8	Up, Operational	1 gbps
☑ Local Area Connection* 9	No	00-00-00-00-00-00	Down, Non Operational	0 bps

Connection: Wired Ethernet Connection 3

8. click random MAC Address to display another Mac address that can be assigned to this device.

9. click the down arrow in the box below the new random Mac address. Note the long list of different NIc vendors from which a Mac address can be chosen.

10. click (2C-30-33) Netgear.



Network Security Textbook.pdf
Technitium MAC Address Changer
https://technitium.com/tmac/
Technitium
Downloads
TMACv6.0.7_Setup.zip
Open file
See more

Technitium MAC Address Changer

A freeware utility to spoof MAC addres

Download Now
Version 6.0.7

Download
Direct Download

Official Torrent
Download Torrent

System Requirements
Windows 10/8.1/8/7/Vista/XP/Server 2012 R2/Server 2012/Server 2008 R2/Server 2003/Server 2000

What's New?
Read this blog post to know what's new in this release.

File Details
Name TMACv6.0.7_Setup.zip
Format ZIP File
Size 2.10 MB
SHA256 6E63BECAF5C5E17A9D3AFB6E2104EEE3DBE473C8930AE8783EBA0FEDADB4A152

Technitium MAC Address Changer v6 - by Shreyas Zare

Network Connections	Changed	MAC Address	Link Status	Speed
☑ Ethernet 2	No	D8-BB-C1-97-3C-68	Up, Operational	100 mbps
☑ Ethernet 3	No	00-FF-F3-A3-E7-18	Up, Non Operational	1 gbps
☑ Radmin VPN	No	02-50-B8-90-31-40	Up, Operational	100 mbps
☑ Ethernet 4	No	0A-00-27-00-00-0D	Up, Operational	1 gbps

Connection Details
Connection: Ethernet 2
Device: Intel(R) Ethernet Controller (3) I225-V #2
Hardware ID: PCI\VEN_8086&DEV_15F3&SUBSYS_7D25146
Config ID: {9ED8DDD7-4398-423C-8270-492F05CDDD58}
TCP/IPv4: Enabled
TCP/IPv6: Enabled
Original MAC Address
D8-BB-C1-97-3C-68
Unknown Vendor
Active MAC Address
D8-BB-C1-97-3C-68 (Original)
Unknown Vendor

Change MAC Address
2C - 30 - 33 - D4 - 95 - 30
Random MAC Address
Address: 350 East Plumeria Drive, San Jose, null, 95134, US

☑ Automatically restart network connection to apply changes
☑ Make new MAC address persistent
☐ Use '02' as first octet of MAC address Why?

Received 154.36 MB (161861404 bytes)
~Speed 1.72 KB/s (1758 bytes)
Sent 114.31 MB (119861479 bytes)
~Speed 1.17 KB/s (1200 bytes)

Technitium MAC Address Changer v6 - by Shreyas Zare

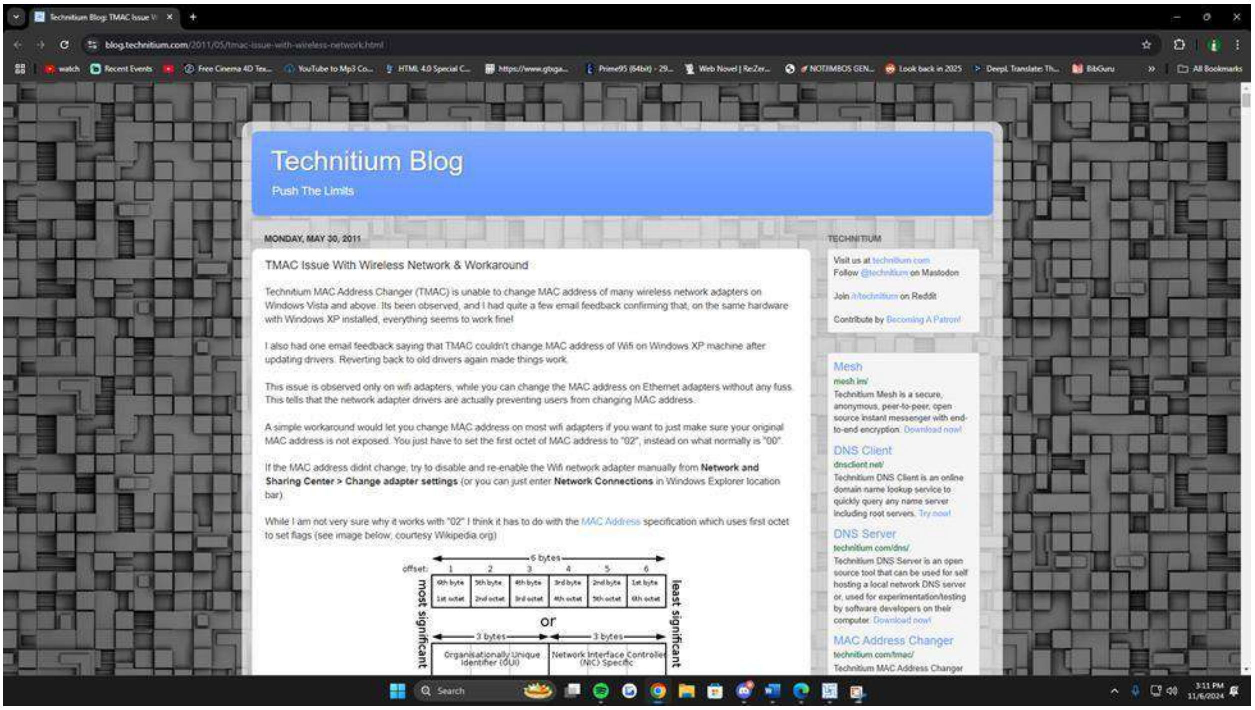
Network Connections	Changed	MAC Address	Link Status	Speed
☑ Wired Ethernet Connection	No	00-0C-29-C3-FC-B1	Up, Non Operational	0 bps
☑ Wired Ethernet Connection 2	No	00-0C-29-C3-FC-BB	Up, Non Operational	0 bps
☑ Wired Ethernet Connection 3	Yes	00-1E-A3-23-9F-D8	Up, Operational	1 gbps
☑ Local Area Connection* 9	No	00-00-00-00-00-00	Down, Non Operational	0 bps

Connection Details
Connection: Wired Ethernet Connection 3
Original MAC Address

11. look at the new Mac address under Change MAC Address and note the first three pairs of numbers. what does this correspond to? **It corresponds to the NIC vendor identifier code**

12. click why? next to use ‘02’ as first octet of MAC address.

13. read the explanation about why 02 should be used as the first octet.



blog.technitium.com/2011/05/tmac-issue-with-wireless-network.html

Technitium Blog

Push The Limits

MONDAY, MAY 30, 2011

TMAC Issue With Wireless Network & Workaround

Technitium MAC Address Changer (TMAC) is unable to change MAC address of many wireless network adapters on Windows Vista and above. Its been observed, and I had quite a few email feedback confirming that, on the same hardware with Windows XP installed, everything seems to work fine!

I also had one email feedback saying that TMAC couldn't change MAC address of Wifi on Windows XP machine after updating drivers. Reverting back to old drivers again made things work.

This issue is observed only on wifi adapters, while you can change the MAC address on Ethernet adapters without any fuss. This tells that the network adapter drivers are actually preventing users from changing MAC address.

A simple workaround would let you change MAC address on most wifi adapters if you want to just make sure your original MAC address is not exposed. You just have to set the first octet of MAC address to "02", instead on what normally is "00".

If the MAC address didnt change, try to disable and re-enable the Wifi network adapter manually from **Network and Sharing Center > Change adapter settings** (or you can just enter **Network Connections** in Windows Explorer location bar).

While I am not very sure why it works with "02" I think it has to do with the MAC Address specification which uses first octet to set flags (see image below, courtesy Wikipedia.org)

TECHNITIUM

Visit us at technitium.com
Follow @technitium on Mastodon

Join /r/technitium on Reddit

Contribute by Becoming A Patron!

Mesh
mesh.im/
Technitium Mesh is a secure, anonymous, peer-to-peer, open source instant messenger with end-to-end encryption. Download now!

DNS Client
dnsclient.net/
Technitium DNS Client is an online domain name lookup service to quickly query any name server including root servers. Try now!

DNS Server
technitium.com/dns/
Technitium DNS Server is an open source tool that can be used for self hosting a local network DNS server or, used for experimentation/testing by software developers on their computer. Download now!

MAC Address Changer
technitium.com/tmac/
Technitium MAC Address Changer

14. If you want to change your Mac address, click Change Now! or close the application if you do not want to change the address.

15. how easy was it to spoof a Mac address? how can a threat actor use this in a Mac cloning attack? **After installing the application, you can change it within seconds each time. Some networks use MAC address filtering as a form of access control, allowing only devices with pre-approved MAC addresses to connect. A threat actor could observe the MAC address of an authorized device and clone it to gain unauthorized access to the network.**

16. close all windows

Case Project 10-1: trustworthy email Protocols and Standards

In addition to S/MIME, there are several protocols and standards that protect email. These include STARTTLS, DNS Based Authentication of Named Entities (DANE), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). Use the Internet to research each of these. Create a summary of each along with the respective strengths and weaknesses. Which would you recommend? Why?

INTRODUCTION

To protect the integrity, authenticity, and confidentiality of emails, several protocols and standards have been developed, each addressing different aspects of email security. These include STARTTLS, DNS-Based Authentication of Named Entities (DANE), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). Together, they form a comprehensive framework to safeguard email transmissions against malicious attacks and ensure that email communication remains trustworthy and secure (Perception Point, 2024).

STARTTLS

STARTTLS is commonly used in email communication, where SMTP servers initiate an encrypted channel for email transmission, and in Internet Relay Chat (IRC), where servers upgrade to secure connections. One of its main advantages is that it enhances data security by encrypting connections. It also offers flexibility by allowing an upgrade from an insecure to a secure connection. However, STARTTLS has drawbacks, including vulnerability to downgrade attacks, where an attacker forces the connection to remain insecure. Additionally, since STARTTLS is optional, some services may still transmit data over unencrypted connections. (NordVPN, 2024)

DNS-Based Authentication of Named Entities (DANE)

DANE strengthens email security by using DNSSEC to bind TLS certificates to domain names, reducing reliance on Certificate Authorities (CAs). This gives domain administrators more control over their security, allowing them to generate their own keys. The main advantage is streamlining trust within the DNS system. Some challenges include the need for expertise in managing CAs, potential security gaps if DNS and security roles are separated, and ongoing risks related to DNSSEC resolver compromises and certificate status checks (Housley C Turner, 2013).

Sender Policy Framework (SPF)

SPF enables domain owners to specify which IP addresses are authorized to send emails on their behalf, thus combating email spoofing. SPF works by checking the sender’s IP address against a published list of allowed servers in DNS. Implementing SPF offers several advantages, such as preventing phishing attacks by flagging emails sent from unauthorized sources and boosting domain reputation by signaling a commitment to email security. However, SPF has some limitations, including the failure of forwarded emails to pass authentication, making it challenging for domain owners to maintain accurate SPF records (DuoCircle, 2023).

DomainKeys Identified Mail (DKIM)

DKIM provides message integrity by allowing the sender's domain to sign an email with a cryptographic key. The recipient can then verify the message was not altered and that it was sent from an authorized source. DKIM ensures the content’s integrity and offers robust protection against certain spoofing attacks, but it can be bypassed by domain abuse or forwarding scenarios, where the signature is no longer valid after transit (Kucherawy, 2011).

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

DMARC is an email authentication protocol that protects against email spoofing and impersonation by using SPF and DKIM standards. It lets domain owners specify how email should be handled when it fails authentication and provides reporting mechanisms to identify failed

authentication attempts. It can prevent phishing attacks and improve domain security by blocking unauthorized use of domain for sending fraud emails. Its effectiveness is based on configuration and doesn’t protect against all types of email-based attacks (Mimecast, 2024).

DMARC is recommended for comprehensive email protection. While each protocol addresses specific threats, DMARC provides a unified approach by leveraging both SPF and DKIM for authentication while offering reporting mechanisms to monitor email activity. Its combination of sender authentication and domain management makes it an effective solution for mitigating email- based attacks, particularly phishing and spoofing, despite the complexity of initial implementation.

References

Cranor, L. (2021). *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc.

DuoCircle. (2023, May 5). *Advantages and Disadvantages of SPF*. Retrieved from DuoCircle: https://support.duocircle.com/support/solutions/articles/5000882462-advantages-and- disadvantages-of-spf

Expert Insights. (2024). *The Top 8 Unified Threat Management Platforms*. Retrieved from https://www.expertinsights.com

Geekflare. (2024). *S Best Unified Threat Management (UTM) Solutions for Small to Big Businesses*.
Retrieved from 9 Best Unified Threat Management (UTM) Solutions for Small to Big Businesses - Geekflare

Housley, R., C Turner, S. (2013, March 12). *The Promise of DANE*. Retrieved from National Institute of Standards and Technology: https://csrc.nist.gov/csrc/media/events/workshop-on- improving-trust-in-the-online- marketpl/documents/submissions/housley_promise_dane.pdf

Kucherawy, M. (2011, September). *DomainKeys Identified Mail (DKIM) and Mailing Lists*. Retrieved from Internet Engineering Task Force: https://www.rfc-editor.org/rfc/pdfrfc/rfc6377.txt.pdf

Assignment 5 – Hands On

Sam Peller

November 27, 2024

ISM 4323

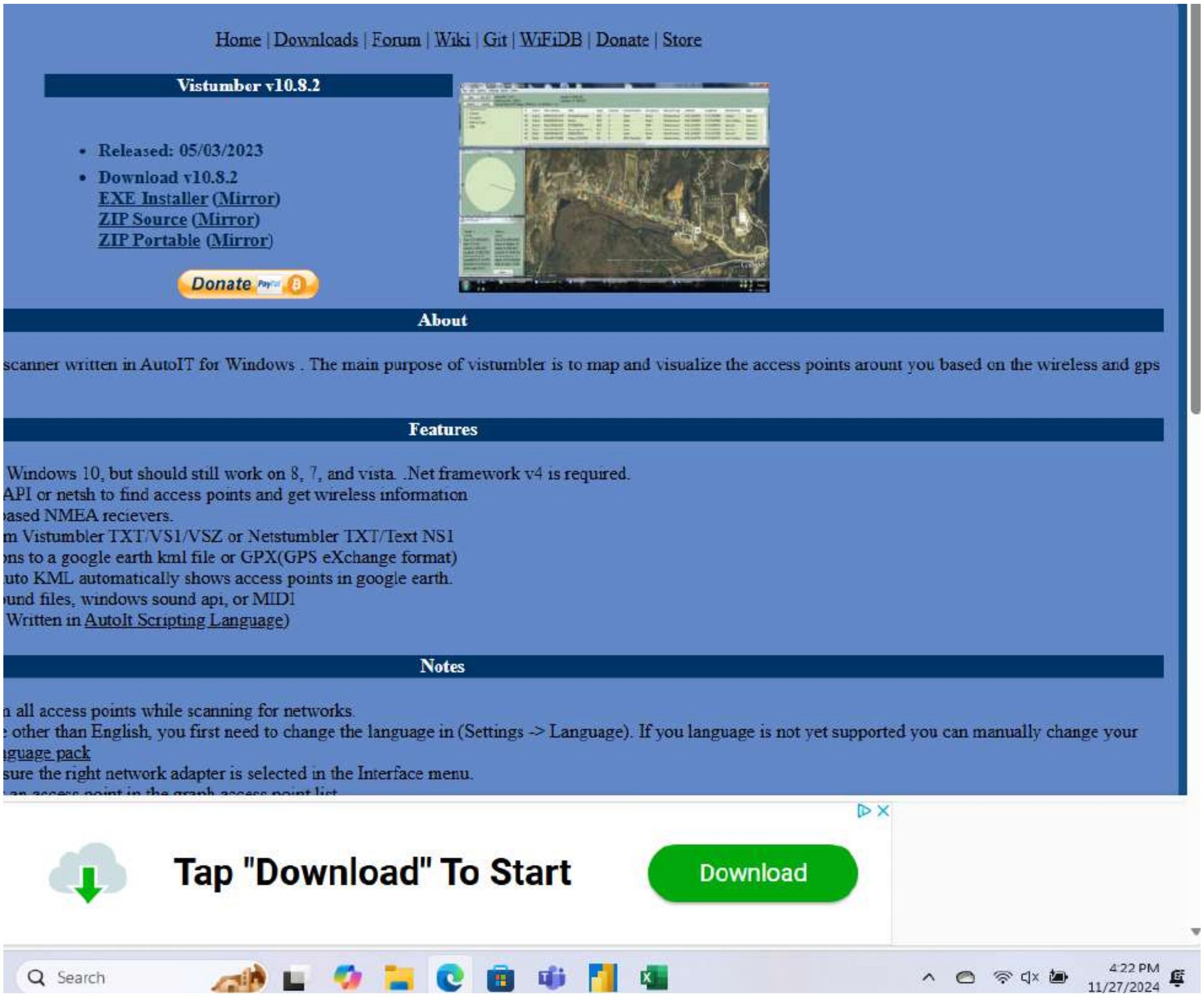
Project 11-2: Viewing WLAN Security Information with Vistumbler

Project 11-2: Viewing WlAN security information with Vistumbler 345
Time required: 25 minutes
Objective: Given a scenario, install and configure wireless security settings.
description: Vistumbler can be used to display the security information that is beaconed out from WLANs. Note that Vistumbler does not allow you to "crack" any WLANs but instead only displays information. In this project, you use Vistumbler to view this information. This project works best when you are in an area in which you can pick up multiple WLAN signals.
Introduction:

Vistumbler is a useful tool for visualizing security information broadcasted by wireless local area networks (WLANs). While it does not provide capabilities for cracking or breaching network security, it is an effective way to gather information about available WLANs, such as their signal strength, encryption types, and other key details. Exploration works particularly well in areas with multiple WLAN signals, allowing for a more diverse set of observations and insights into network characteristics and coverage.

1. Use your web browser to go to www.vistumbler.net. (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine and

search for “Vistumbler.”)


Home | Downloads | Forum | Wiki | Git | WiFiDB | Donate | Store

Vistumber v10.8.2

- Released: 05/03/2023
- Download v10.8.2
  EXE Installer (Mirror)
  ZIP Source (Mirror)
  ZIP Portable (Mirror)

About

scanner written in AutoIT for Windows . The main purpose of vistumbler is to map and visualize the access points arount you based on the wireless and gps

Features

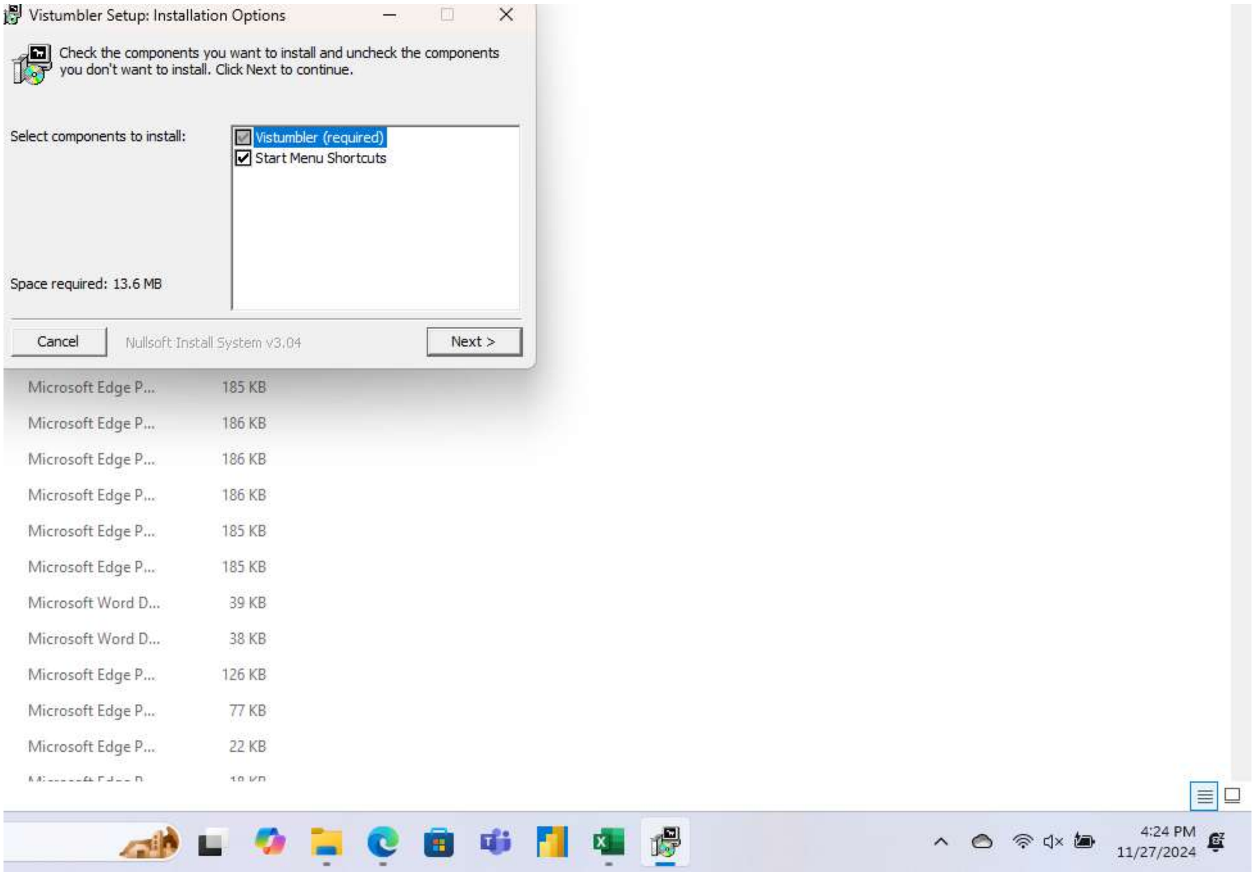
Windows 10, but should still work on 8, 7, and vista. .Net framework v4 is required.
API or netsh to find access points and get wireless information
ased NMEA recievers.
m Vistumbler TXT/VS1/VSZ or Netstumbler TXT/Text NS1
ons to a google earth kml file or GPX(GPS eXchange format)
uto KML automatically shows access points in google earth.
und files, windows sound api, or MIDI
Written in AutoIt Scripting Language)

Notes

n all access points while scanning for networks.
other than English, you first need to change the language in (Settings -> Language). If you language is not yet supported you can manually change your
guage pack
sure the right network adapter is selected in the Interface menu.
an access point in the graph access point list

2. Click eXe Installer (Mirror).

3. Follow the prompts to download and install Vistumbler using the default settings



Vistumbler Setup: Installation Options

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Vistumbler (required)

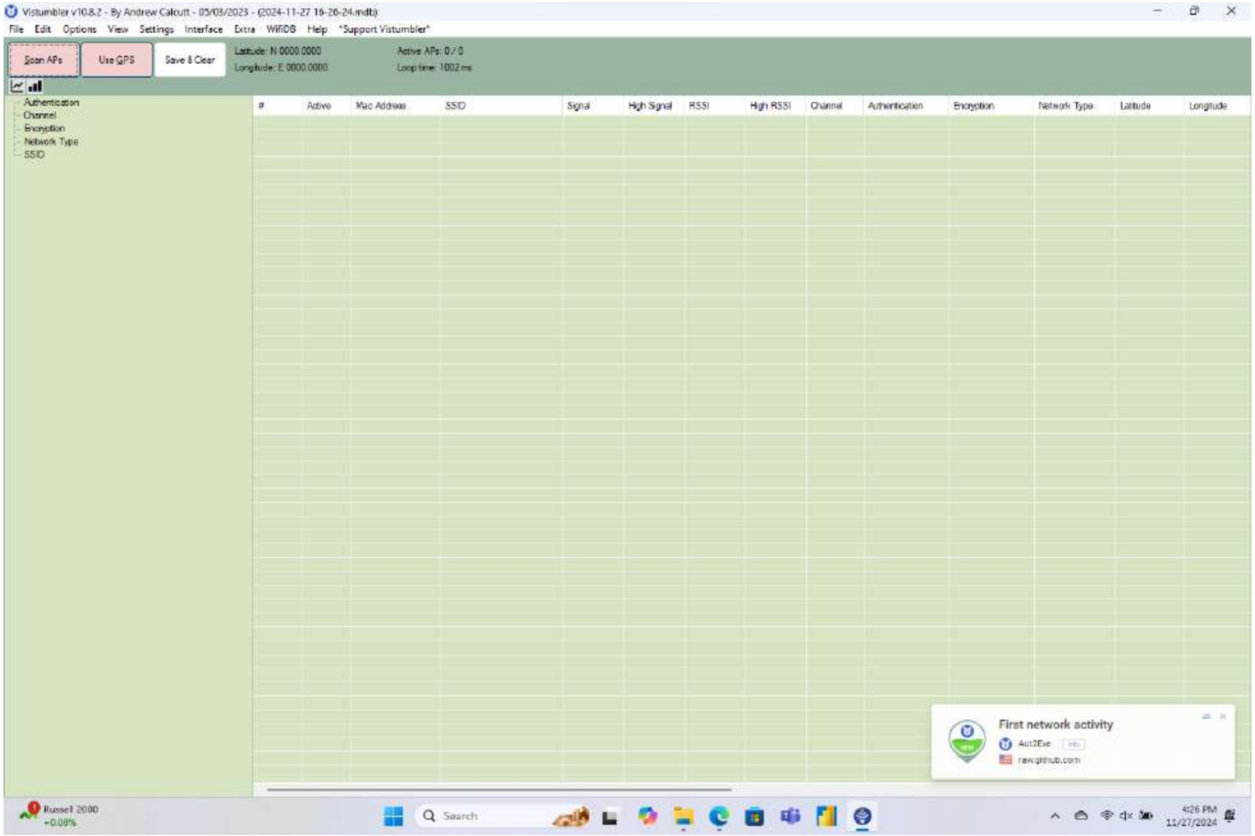
☑ Start Menu Shortcuts

Space required: 13.6 MB

Microsoft Edge P...	185 KB
Microsoft Edge P...	186 KB
Microsoft Edge P...	186 KB
Microsoft Edge P...	186 KB
Microsoft Edge P...	185 KB
Microsoft Edge P...	185 KB
Microsoft Word D...	39 KB
Microsoft Word D...	38 KB
Microsoft Edge P...	126 KB
Microsoft Edge P...	77 KB
Microsoft Edge P...	22 KB

4. If the program does not start after the installation is complete, launch Vistumbler.

5. If necessary, expand the window to full screen



Vistumbler v10.8.2 - By Andrew Calcutt - 05/03/2023 - (2024-11-27 16-26-24.mdb)

Latitude: N 0000.0000

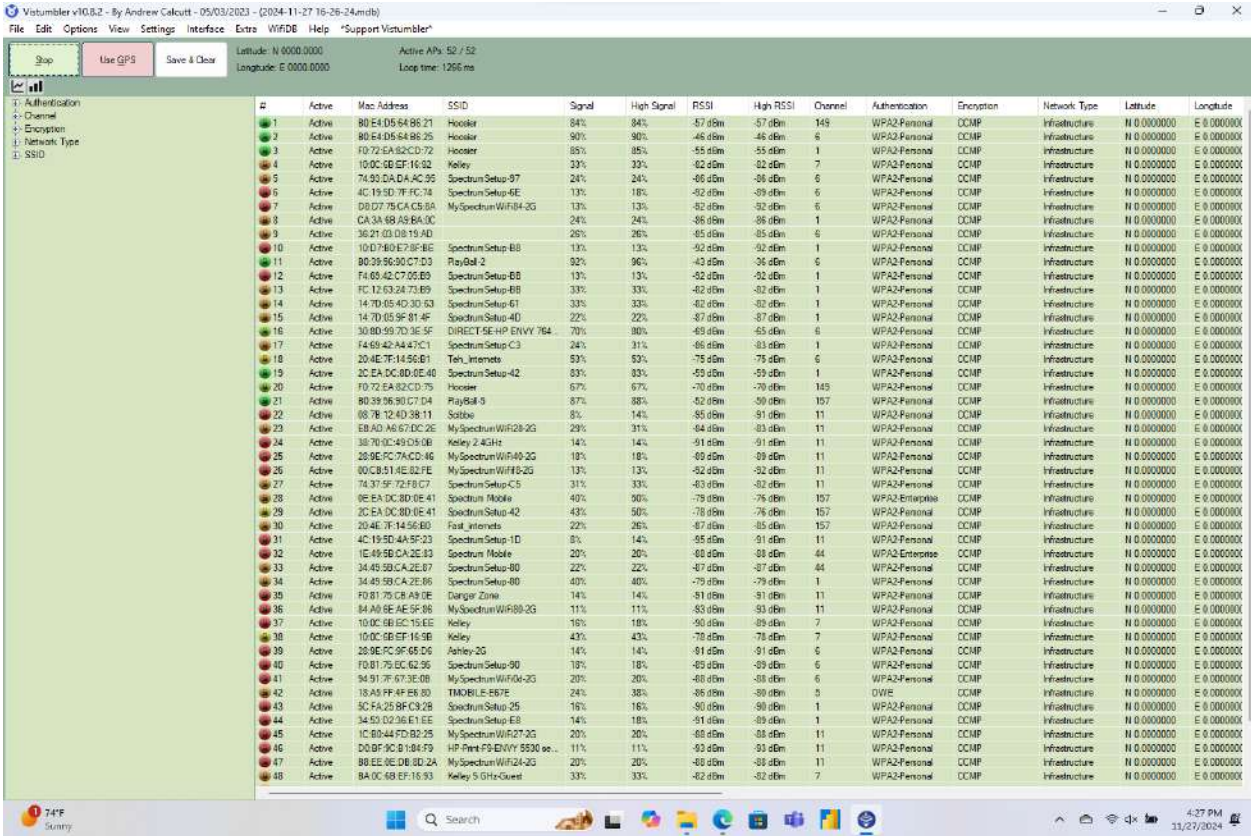
Longitude: E 0000.0000

Active APs: 0 / 0

Loop time: 1002 ms

#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude

6. Click Scan APs. If no networks appear, click Interface and then select the appropriate wireless NIC interface.



Latitude: N 0000.0000
Longitude: E 0000.0000

Active APs: 52 / 52
Loop time: 1266 ms

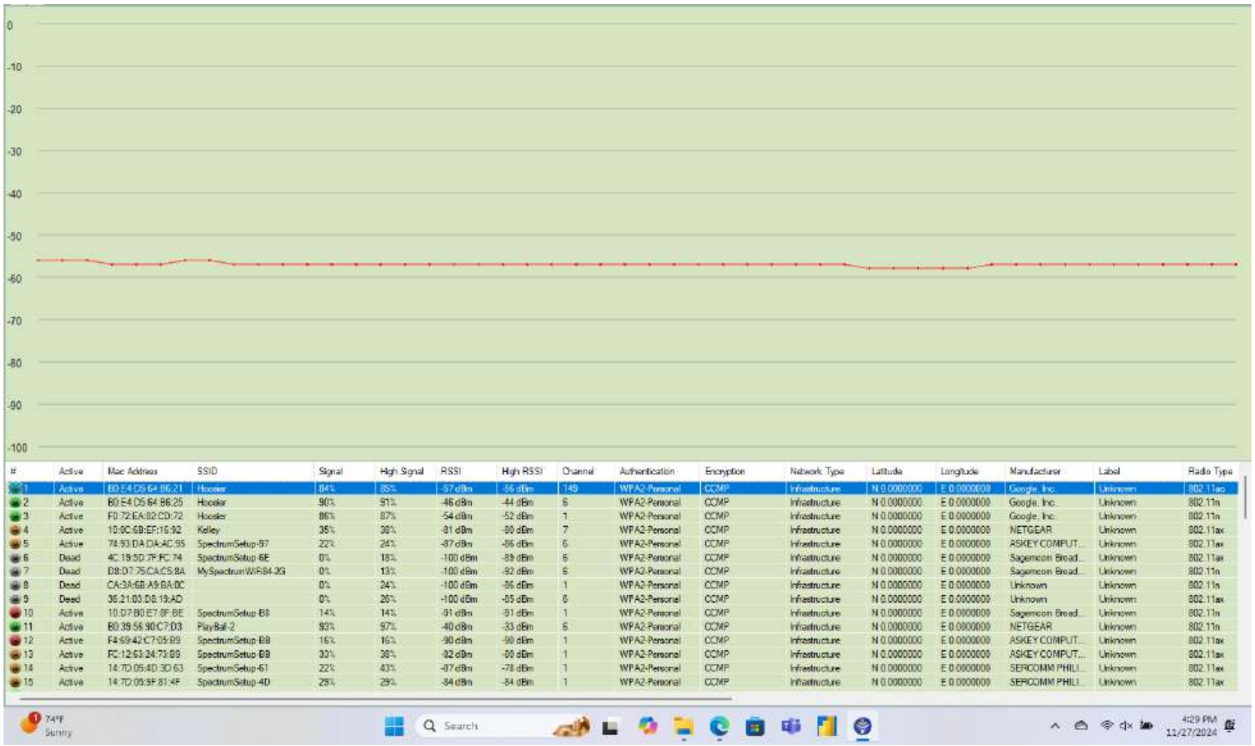
#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude
1	Active	80:E4:D5:64:B6:21	Hoosier	84%	84%	-57 dBm	-57 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
2	Active	80:E4:D5:64:B6:25	Hoosier	90%	90%	-46 dBm	-46 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
3	Active	F0:72:EA:82:CD:72	Hoosier	85%	85%	-55 dBm	-55 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
4	Active	10:0C:6B:EF:16:92	Kelley	33%	33%	-82 dBm	-82 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
5	Active	74:93:DA:DA:AC:95	SpectrumSetup-97	24%	24%	-86 dBm	-86 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
6	Active	4C:19:5D:7F:FC:74	SpectrumSetup-6E	13%	18%	-92 dBm	-89 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
7	Active	D8:D7:75:CA:C5:8A	MySpectrumWiFi84-2G	13%	13%	-92 dBm	-92 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
8	Active	CA:3A:6B:A9:BA:0C		24%	24%	-86 dBm	-86 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
9	Active	36:21:03:D8:19:AD		26%	26%	-85 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
10	Active	10:D7:B0:E7:8F:BE	SpectrumSetup-B8	13%	13%	-92 dBm	-92 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
11	Active	80:39:56:90:C7:D3	PlayBall-2	92%	96%	-43 dBm	-36 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
12	Active	F4:69:42:C7:05:B9	SpectrumSetup-B8	13%	13%	-92 dBm	-92 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
13	Active	FC:12:63:24:73:B9	SpectrumSetup-B8	33%	33%	-82 dBm	-82 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
14	Active	14:7D:05:4D:30:63	SpectrumSetup-61	33%	33%	-82 dBm	-82 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
15	Active	14:7D:05:9F:81:4F	SpectrumSetup-4D	22%	22%	-87 dBm	-87 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
16	Active	30:8D:99:7D:3E:5F	DIRECT-5E-HP ENVY 764 ...	70%	80%	-69 dBm	-65 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
17	Active	F4:69:42:A4:47:C1	SpectrumSetup-C3	24%	31%	-86 dBm	-83 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
18	Active	20:4E:7F:14:56:B1	Teh_Internets	53%	53%	-75 dBm	-75 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
19	Active	2C:EA:DC:8D:0E:40	SpectrumSetup-42	83%	83%	-59 dBm	-59 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
20	Active	F0:72:EA:82:CD:75	Hoosier	67%	67%	-70 dBm	-70 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
21	Active	80:39:56:90:C7:D4	PlayBall-5	87%	88%	-52 dBm	-50 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
22	Active	08:7B:12:4D:38:11	Sobbe	8%	14%	-95 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
23	Active	E8:AD:A6:67:DC:2E	MySpectrumWiFi28-2G	29%	31%	-84 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
24	Active	38:70:0C:49:D5:0B	Kelley 2.4GHz	14%	14%	-91 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
25	Active	28:9E:FC:7A:CD:46	MySpectrumWiFi40-2G	18%	18%	-89 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
26	Active	00:CB:51:4E:82:FE	MySpectrumWiFif8-2G	13%	13%	-92 dBm	-92 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
27	Active	74:37:5F:72:F8:C7	SpectrumSetup-C5	31%	33%	-83 dBm	-82 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
28	Active	0E:EA:DC:8D:0E:41	Spectrum Mobile	40%	50%	-79 dBm	-76 dBm	157	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
29	Active	2C:EA:DC:8D:0E:41	SpectrumSetup-42	43%	50%	-78 dBm	-76 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
30	Active	20:4E:7F:14:56:B0	Fast_internets	22%	26%	-87 dBm	-85 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
31	Active	4C:19:5D:4A:5F:23	SpectrumSetup-1D	8%	14%	-95 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
32	Active	1E:49:5B:CA:2E:83	Spectrum Mobile	20%	20%	-88 dBm	-88 dBm	44	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
33	Active	34:49:5B:CA:2E:87	SpectrumSetup-80	22%	22%	-87 dBm	-87 dBm	44	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
34	Active	34:49:5B:CA:2E:86	SpectrumSetup-80	40%	40%	-79 dBm	-79 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
35	Active	F0:81:75:CB:A9:0E	Danger Zone	14%	14%	-91 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
36	Active	84:A0:6E:AE:5F:86	MySpectrumWiFi80-2G	11%	11%	-93 dBm	-93 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
37	Active	10:0C:6B:EC:15:EE	Kelley	16%	18%	-90 dBm	-89 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
38	Active	10:0C:6B:EF:16:9B	Kelley	43%	43%	-78 dBm	-78 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
39	Active	28:9E:FC:9F:65:D6	Ashley-2G	14%	14%	-91 dBm	-91 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
40	Active	F0:81:75:EC:62:96	SpectrumSetup-90	18%	18%	-89 dBm	-89 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
41	Active	94:91:7F:67:3E:08	MySpectrumWiFi0d-2G	20%	20%	-88 dBm	-88 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
42	Active	18:A5:FF:4F:E6:80	TMOBILE-E67E	24%	38%	-86 dBm	-80 dBm	5	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
43	Active	5C:FA:25:BF:C9:2B	SpectrumSetup-25	16%	16%	-90 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
44	Active	34:53:D2:36:E1:EE	SpectrumSetup-E8	14%	18%	-91 dBm	-89 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
45	Active	1C:B0:44:FD:B2:25	MySpectrumWiFi27-2G	20%	20%	-88 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
46	Active	D0:BF:9C:B1:84:F9	HP-Print-F9-ENVY 5530 se...	11%	11%	-93 dBm	-93 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
47	Active	B8:EE:0E:DB:8D:2A	MySpectrumWiFi24-2G	20%	20%	-88 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
48	Active	BA:0C:6B:EF:16:93	Kelley 5 GHz-Guest	33%	33%	-82 dBm	-82 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000

7. Note the columns Signal and High Signal. How could they be used in a site survey?

In a site survey, the "Signal" and "High Signal" columns help assess wireless signal strength and quality throughout an area. The "Signal" column shows the strength of the wireless signal, helping identify weak coverage areas that may need more access points or adjustments. The "High Signal" column indicates areas with strong coverage, useful for ensuring key locations have reliable connectivity. Comparing these columns helps identify signal fluctuations or interference, guiding decisions on optimizing access point placement. Together, they ensure consistent and effective wireless coverage across the site.

8. Click Graph 1.

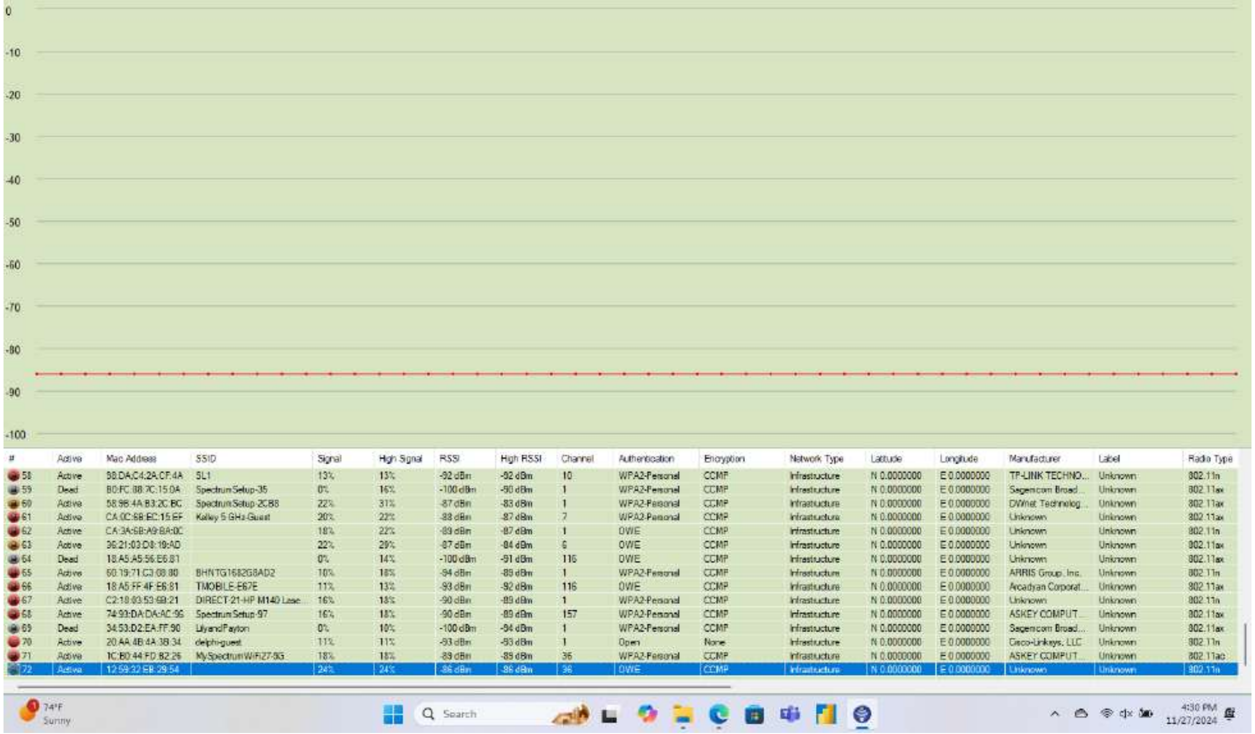
9. Click one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes. What information is displayed on this graph?



#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude	Manufacturer	Label	Radio Type
1	Active	B0:E4:D5:64:B6:21	Hoosier	84%	85%	-57 dBm	-56 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Google, Inc.	Unknown	802.11ac
2	Active	B0:E4:D5:64:B6:25	Hoosier	90%	91%	-46 dBm	-44 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Google, Inc.	Unknown	802.11n
3	Active	F0:72:EA:82:CD:72	Hoosier	86%	87%	-54 dBm	-52 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Google, Inc.	Unknown	802.11n
4	Active	10:0C:6B:EF:16:92	Kelley	35%	38%	-81 dBm	-80 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	NETGEAR	Unknown	802.11ax
5	Active	74:93:DA:DA:AC:95	SpectrumSetup-97	22%	24%	-87 dBm	-86 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ASKEY COMPUT...	Unknown	802.11ax
6	Dead	4C:19:5D:7F:FC:74	SpectrumSetup-6E	0%	18%	-100 dBm	-89 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Sagemcom Broad...	Unknown	802.11ax
7	Dead	D8:D7:75:CA:C5:8A	MySpectrumWiFi84-2G	0%	13%	-100 dBm	-92 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Sagemcom Broad...	Unknown	802.11n
8	Dead	CA:3A:6B:A9:BA:0C		0%	24%	-100 dBm	-86 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
9	Dead	36:21:03:D8:19:AD		0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ax
10	Active	10:D7:B0:E7:8F:BE	SpectrumSetup-B8	14%	14%	-91 dBm	-91 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Sagemcom Broad...	Unknown	802.11n
11	Active	B0:39:56:90:C7:D3	PlayBall-2	93%	97%	-40 dBm	-33 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	NETGEAR	Unknown	802.11n
12	Active	F4:69:42:C7:05:B9	SpectrumSetup-B8	16%	16%	-90 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ASKEY COMPUT...	Unknown	802.11ax
13	Active	FC:12:63:24:73:B9	SpectrumSetup-B8	33%	38%	-82 dBm	-80 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ASKEY COMPUT...	Unknown	802.11ax
14	Active	14:7D:05:4D:3D:63	SpectrumSetup-61	22%	43%	-87 dBm	-78 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	SERCOMM PHILI...	Unknown	802.11ax
15	Active	14:7D:05:9F:81:4F	SpectrumSetup-4D	29%	29%	-84 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	SERCOMM PHILI...	Unknown	802.11ax

10. Click Graph 2.

11. Click another one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes. What information is displayed on this graph? How is this different from the previous graph?



#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude	Manufacturer	Label	Radio Type
58	Active	98:DA:C4:2A:CF:4A	SL1	13%	13%	-92 dBm	-92 dBm	10	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK TECHNO...	Unknown	802.11n
59	Dead	B0:FC:88:7C:15:0A	SpectrumSetup-35	0%	16%	-100 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Sagemcom Broad...	Unknown	802.11ax
60	Active	58:96:4A:B3:2C:BC	SpectrumSetup-2CB8	22%	31%	-87 dBm	-83 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	DWnet Technolog...	Unknown	802.11ax
61	Active	CA:0C:6B:EC:15:EF	Kelley 5 GHz-Guest	20%	22%	-88 dBm	-87 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ax
62	Active	CA:3A:6B:A9:BA:0C		18%	22%	-89 dBm	-87 dBm	1	OWE	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
63	Active	36:21:03:D8:19:AD		22%	29%	-87 dBm	-84 dBm	6	OWE	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ax
64	Dead	18:A5:A5:56:E6:81		0%	14%	-100 dBm	-91 dBm	116	OWE	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11ax
65	Active	60:19:71:C3:08:80	BHNTG1682G8AD2	10%	18%	-94 dBm	-89 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ARRIS Group, Inc.	Unknown	802.11n
66	Active	18:A5:FF:4F:E6:81	TMOBILE-E67E	11%	13%	-93 dBm	-92 dBm	116	OWE	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Arcadyan Corporat...	Unknown	802.11ax
67	Active	C2:18:03:53:6B:21	DIRECT-21-HP M140 Lase...	16%	18%	-90 dBm	-89 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n
68	Active	74:93:DA:DA:AC:96	SpectrumSetup-97	16%	18%	-90 dBm	-89 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ASKEY COMPUT...	Unknown	802.11ax
69	Dead	34:53:D2:EA:FF:90	LilyandPayton	0%	10%	-100 dBm	-94 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Sagemcom Broad...	Unknown	802.11ax
70	Active	20:AA:4B:4A:3B:34	delphi-guest	11%	11%	-93 dBm	-93 dBm	1	Open	None	Infrastructure	N 0.0000000	E 0.0000000	Cisco-Linksys, LLC	Unknown	802.11n
71	Active	1C:B0:44:FD:B2:26	MySpectrumWiFi27-5G	18%	18%	-89 dBm	-89 dBm	36	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	ASKEY COMPUT...	Unknown	802.11ac
72	Active	12:59:32:EB:29:54		24%	24%	-86 dBm	-86 dBm	36	OWE	CCMP	Infrastructure	N 0.0000000	E 0.0000000	Unknown	Unknown	802.11n

12. Click No Graph to return to the previous screen.

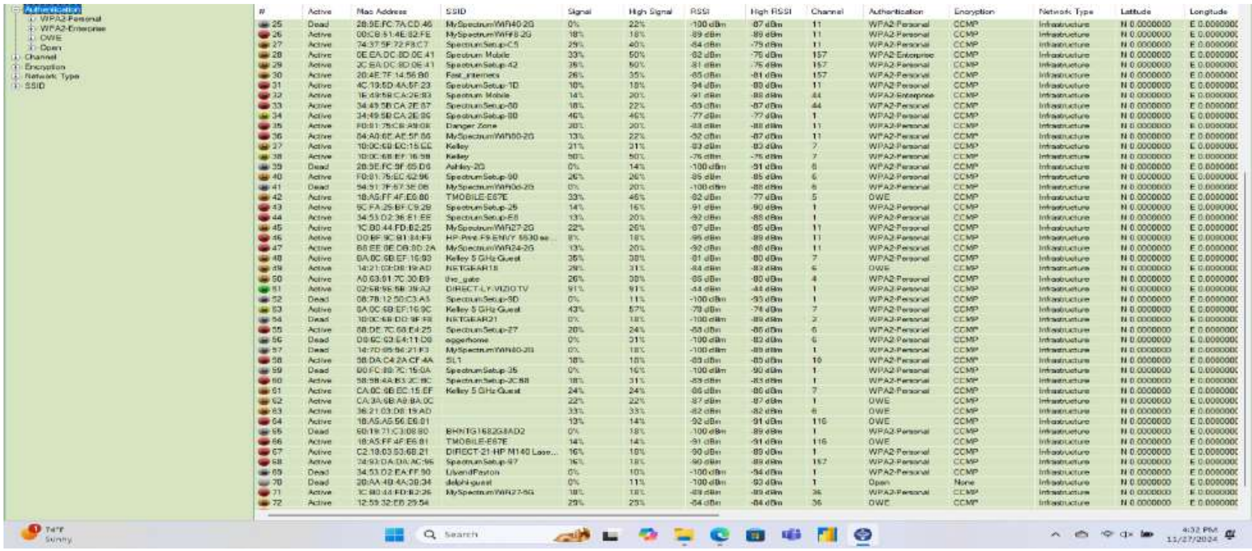
13. Use the horizontal scroll bar to move to the right. Note the columns Authentication, encryption, Manufacturer, and radio Type. How would this information be useful to an attacker?

They provide critical information that could be exploited by an attacker. The "Authentication" and "Encryption" columns reveal the security protocols in use, such as WPA2 or WEP, allowing an attacker to identify weaker security methods that are more susceptible to attacks, like cracking WEP keys. The

"Manufacturer" column can provide insight into the type of devices being used, which helps an attacker target known vulnerabilities specific to that brand. Finally, the "Radio Type" column provides details on the wireless standard (e.g., 802.11n, 802.11ac), which could help an attacker determine potential attack methods or limitations of the network. Together, this information allows an attacker to identify weak points in the network and tailor their approach for gaining unauthorized access.

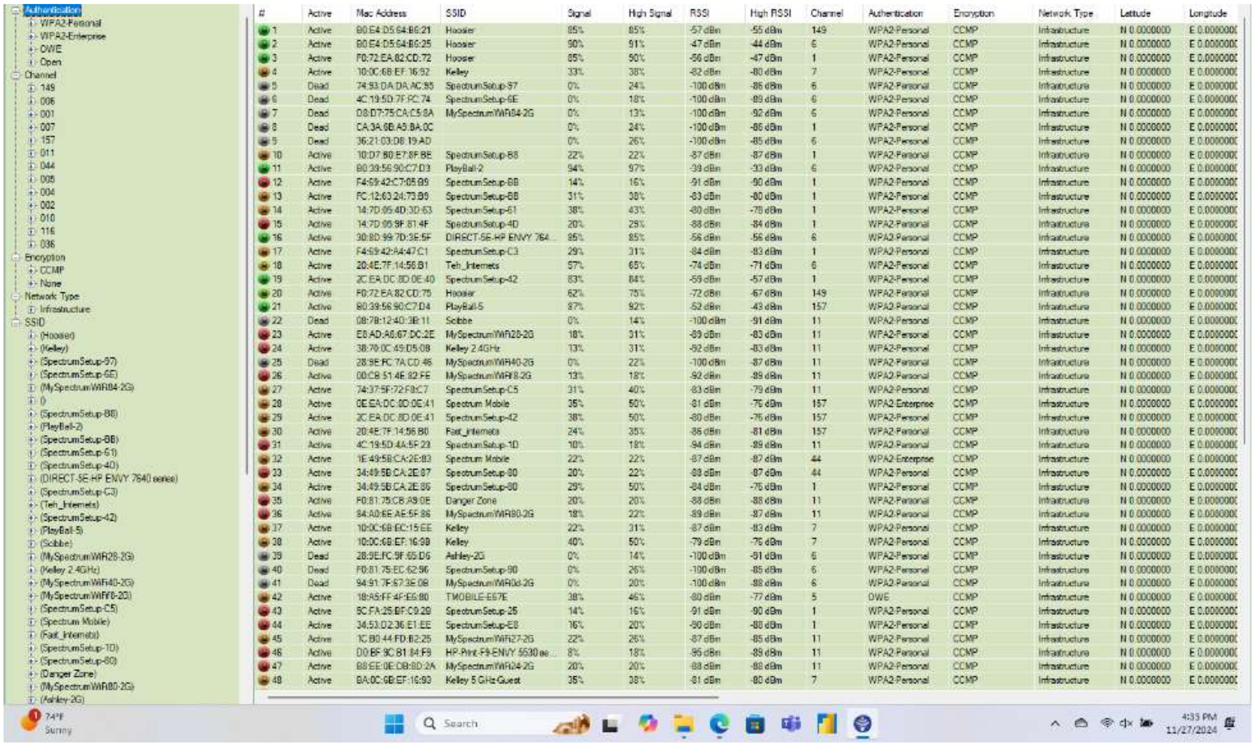
14. Use the horizontal scroll bar to move back to the far left.

15. In the left pane, expand the information under Authentication. What types are listed?



#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude
25	Dead	28:9E:FC:7A:CD:46	MySpectrumWiFi40-2G	0%	22%	-100 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
26	Active	00:C8:51:4E:82:FE	MySpectrumWiFi8-2G	18%	18%	-89 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
27	Active	74:37:5F:72:F8:C7	SpectrumSetup-C5	29%	40%	-84 dBm	-79 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
28	Active	0E:EA:DC:8D:0E:41	Spectrum Mobile	33%	50%	-82 dBm	-76 dBm	157	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
29	Active	2C:EA:DC:8D:0E:41	SpectrumSetup-42	35%	50%	-81 dBm	-76 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
30	Active	20:4E:7F:14:56:B0	Fast_internets	26%	35%	-85 dBm	-81 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
31	Active	4C:19:5D:4A:5F:23	SpectrumSetup-1D	10%	18%	-94 dBm	-80 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
32	Active	1E:49:5B:CA:2E:83	Spectrum Mobile	14%	20%	-91 dBm	-88 dBm	44	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
33	Active	34:49:5B:CA:2E:87	SpectrumSetup-80	18%	22%	-83 dBm	-87 dBm	44	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
34	Active	34:49:5B:CA:2E:86	SpectrumSetup-80	46%	46%	-77 dBm	-77 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
35	Active	F0:81:75:C8:A9:0E	Danger Zone	20%	20%	-88 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
36	Active	84:A0:6E:AE:5F:86	MySpectrumWiFi80-2G	13%	22%	-92 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
37	Active	10:0C:6B:EC:15:EE	Kelley	21%	31%	-83 dBm	-83 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
38	Active	10:0C:6B:EF:16:98	Kelley	50%	50%	-76 dBm	-75 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
39	Dead	28:9E:FC:9F:65:D6	Ashley-2G	0%	14%	-100 dBm	-91 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
40	Active	F0:81:75:EC:62:96	SpectrumSetup-90	26%	26%	-85 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
41	Dead	94:91:7F:67:3E:08	MySpectrumWiFi0d-2G	0%	20%	-100 dBm	-88 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
42	Active	18:A5:FF:4F:E6:80	TMOBILE-E67E	33%	46%	-82 dBm	-77 dBm	5	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
43	Active	5C:FA:25:BF:C9:28	SpectrumSetup-25	14%	16%	-91 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
44	Active	34:53:D2:36:E1:EE	SpectrumSetup-E8	13%	20%	-92 dBm	-88 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
45	Active	1C:B0:44:FD:82:25	MySpectrumWiFi27-2G	22%	26%	-87 dBm	-85 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
46	Active	00:BF:9C:81:84:F9	HP-Print-F9-ENVY 5530 se...	8%	18%	-96 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
47	Active	B8:EE:0E:DB:8D:2A	MySpectrumWiFi24-2G	13%	20%	-92 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
48	Active	BA:0C:6B:EF:16:93	Kelley 5 GHz Guest	35%	38%	-81 dBm	-80 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
49	Active	14:21:03:D8:19:AD	NETGEAR18	29%	31%	-84 dBm	-83 dBm	6	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
50	Active	A0:63:91:7C:30:B9	the_gate	26%	38%	-85 dBm	-80 dBm	4	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
51	Active	02:68:96:6B:39:A2	DIRECT-LY-VIZIOTV	91%	91%	-44 dBm	-44 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
52	Dead	08:7B:12:50:C3:A5	SpectrumSetup-9D	0%	11%	-100 dBm	-93 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
53	Active	8A:0C:6B:EF:16:9C	Kelley 5 GHz Guest	43%	57%	-70 dBm	-74 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
54	Dead	10:0C:6B:DD:9F:F8	NETGEAR21	0%	18%	-100 dBm	-89 dBm	2	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
55	Active	88:DE:7C:68:E4:25	SpectrumSetup-27	20%	24%	-88 dBm	-86 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
56	Dead	D8:6C:63:E4:11:D8	eggerhome	0%	31%	-100 dBm	-82 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
57	Dead	14:7D:05:94:21:F3	MySpectrumWiFi60-2G	0%	18%	-100 dBm	-89 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
58	Active	58:DA:C4:2A:CF:4A	SL1	18%	18%	-83 dBm	-85 dBm	10	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
59	Dead	00:FC:8D:7C:15:0A	SpectrumSetup-35	0%	16%	-100 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
60	Active	58:98:4A:B3:2C:8C	SpectrumSetup-2C88	18%	31%	-83 dBm	-83 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
61	Active	CA:0C:6B:EC:15:EF	Kelley 5 GHz Guest	24%	24%	-86 dBm	-86 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
62	Active	CA:3A:6B:A8:BA:0C		22%	22%	-87 dBm	-87 dBm	1	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
63	Active	36:21:03:D8:19:AD		33%	33%	-82 dBm	-82 dBm	6	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
64	Active	18:A5:A5:56:E6:81		13%	14%	-92 dBm	-91 dBm	116	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
65	Dead	60:19:71:C3:08:80	BHNTG1682G8AD2	0%	18%	-100 dBm	-89 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
66	Active	18:A5:FF:4F:E6:81	TMOBILE-E67E	14%	14%	-91 dBm	-91 dBm	116	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
67	Active	C2:18:03:53:6B:21	DIRECT-21-HP M140 Lase...	16%	18%	-90 dBm	-89 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
68	Active	74:93:DA:DA:AC:96	SpectrumSetup-97	16%	18%	-90 dBm	-89 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
69	Dead	34:53:D2:EA:FF:90	LilyandPaxton	0%	10%	-100 dBm	-94 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
70	Dead	20:AA:4B:4A:38:34	delphi-guest	0%	11%	-100 dBm	-93 dBm	1	Open	None	Infrastructure	N 0.0000000	E 0.000000
71	Active	1C:B0:44:FD:82:26	MySpectrumWiFi27-5G	18%	18%	-89 dBm	-89 dBm	36	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
72	Active	12:59:32:EB:29:54		29%	25%	-84 dBm	-84 dBm	36	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000

16. Expand the information under these types and note the information given for the wireless LAN signals.

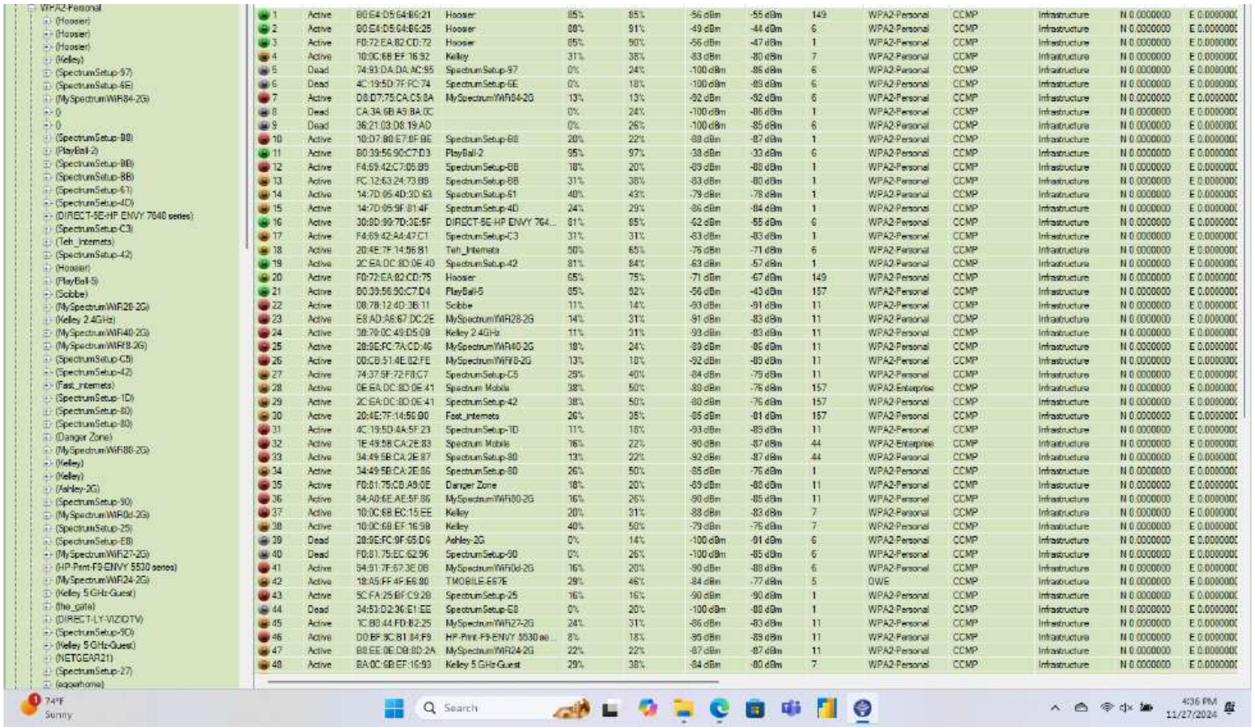


#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitude
1	Active	B0:E4:D5:64:B6:21	Hoosier	85%	85%	-57 dBm	-55 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
2	Active	B0:E4:D5:64:B6:25	Hoosier	90%	91%	-47 dBm	-44 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
3	Active	F0:72:EA:82:CD:72	Hoosier	85%	90%	-56 dBm	-47 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
4	Active	10:0C:6B:EF:16:92	Kelley	33%	38%	-82 dBm	-80 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
5	Dead	74:93:DA:DA:AC:95	SpectrumSetup-97	0%	24%	-100 dBm	-86 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
6	Dead	4C:19:5D:7F:FC:74	SpectrumSetup-6E	0%	18%	-100 dBm	-89 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
7	Dead	D8:D7:75:CA:C5:8A	MySpectrumWiFi84-2G	0%	13%	-100 dBm	-92 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
8	Dead	CA:3A:6B:A5:BA:0C		0%	24%	-100 dBm	-86 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
9	Dead	36:21:03:D8:19:AD		0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
10	Active	10:D7:B0:E7:8F:BE	SpectrumSetup-B8	22%	22%	-87 dBm	-87 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
11	Active	B0:39:56:90:C7:D3	PlayBall-2	94%	97%	-39 dBm	-33 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
12	Active	F4:69:42:C7:05:B9	SpectrumSetup-BB	14%	16%	-91 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
13	Active	FC:12:63:24:73:B9	SpectrumSetup-BB	31%	38%	-83 dBm	-80 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
14	Active	14:7D:05:4D:3D:63	SpectrumSetup-61	38%	43%	-80 dBm	-78 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
15	Active	14:7D:05:9F:81:4F	SpectrumSetup-4D	20%	29%	-88 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
16	Active	30:8D:99:7D:3E:5F	DIRECT-5E-HP ENVY 764...	85%	85%	-56 dBm	-56 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
17	Active	F4:69:42:A4:47:C1	SpectrumSetup-C3	29%	31%	-84 dBm	-83 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
18	Active	20:4E:7F:14:56:B1	Teh_Internets	57%	65%	-74 dBm	-71 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
19	Active	2C:EA:DC:8D:0E:40	SpectrumSetup-42	83%	84%	-59 dBm	-57 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
20	Active	F0:72:EA:82:CD:75	Hoosier	62%	75%	-72 dBm	-67 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
21	Active	B0:39:56:90:C7:D4	PlayBall-5	87%	92%	-52 dBm	-43 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
22	Dead	08:7B:12:40:3B:11	Scibbe	0%	14%	-100 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
23	Active	E8:AD:A6:67:DC:2E	MySpectrumWiFi28-2G	18%	31%	-89 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
24	Active	38:70:0C:49:D5:08	Kelley 2.4GHz	13%	31%	-92 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
25	Dead	28:9E:FC:7A:CD:46	MySpectrumWiFi40-2G	0%	22%	-100 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
26	Active	00:C8:51:4E:82:FE	MySpectrumWiFi8-2G	13%	18%	-92 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
27	Active	74:37:5F:72:F8:C7	SpectrumSetup-C5	31%	40%	-83 dBm	-79 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
28	Active	0E:EA:DC:8D:0E:41	Spectrum Mobile	35%	50%	-81 dBm	-76 dBm	157	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
29	Active	2C:EA:DC:8D:0E:41	SpectrumSetup-42	38%	50%	-80 dBm	-76 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
30	Active	20:4E:7F:14:56:B0	Fast_internets	24%	35%	-86 dBm	-81 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
31	Active	4C:19:5D:4A:5F:23	SpectrumSetup-1D	10%	18%	-94 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
32	Active	1E:49:5B:CA:2E:83	Spectrum Mobile	22%	22%	-87 dBm	-87 dBm	44	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
33	Active	34:49:5B:CA:2E:87	SpectrumSetup-80	20%	22%	-88 dBm	-87 dBm	44	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
34	Active	34:49:5B:CA:2E:86	SpectrumSetup-80	29%	50%	-84 dBm	-76 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
35	Active	F0:81:75:C8:A9:0E	Danger Zone	20%	20%	-88 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
36	Active	84:A0:6E:AE:5F:86	MySpectrumWiFi80-2G	18%	22%	-89 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
37	Active	10:0C:6B:EC:15:EE	Kelley	22%	31%	-87 dBm	-83 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
38	Active	10:0C:6B:EF:16:98	Kelley	40%	50%	-79 dBm	-76 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
39	Dead	28:9E:FC:9F:65:D6	Ashley-2G	0%	14%	-100 dBm	-91 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
40	Dead	F0:81:75:EC:62:96	SpectrumSetup-90	0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
41	Dead	94:91:7F:67:3E:08	MySpectrumWiFi0d-2G	0%	20%	-100 dBm	-88 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
42	Active	18:A5:FF:4F:E6:80	TMOBILE-E67E	38%	46%	-80 dBm	-77 dBm	5	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
43	Active	5C:FA:25:BF:C9:28	SpectrumSetup-25	14%	16%	-91 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
44	Active	34:53:D2:36:E1:EE	SpectrumSetup-E8	16%	20%	-90 dBm	-88 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
45	Active	1C:B0:44:FD:82:25	MySpectrumWiFi27-2G	22%	26%	-87 dBm	-85 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
46	Active	00:BF:9C:81:84:F9	HP-Print-F9-ENVY 5530 se...	8%	18%	-96 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
47	Active	B8:EE:0E:DB:8D:2A	MySpectrumWiFi24-2G	20%	20%	-88 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
48	Active	BA:0C:6B:EF:16:93	Kelley 5 GHz Guest	35%	38%	-81 dBm	-80 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000

17. In the left pane, expand the information under encryption. What types are listed? Which types are most secure? Which types are least secure?

types like WEP, WPA, WPA2, are listed. WPA2, then WPA is less secure, while WEP is the least secure and highly vulnerable. It is best to use WPA3 or WPA2 and avoid WEP and WPA.

18. Expand the information under these types and note the information given for each WLAN.



WPA2-Personal
(Hoosier)
(Hoosier)
(Hoosier)
(Kelley)
(SpectrumSetup-97)
(SpectrumSetup-6E)
(MySpectrumWiFi84-2G)
()
()
(SpectrumSetup-B8)
(PlayBall-2)
(SpectrumSetup-8B)
(SpectrumSetup-8B)
(SpectrumSetup-61)
(SpectrumSetup-4D)
(DIRECT-5E-HP ENVY 7640 series)
(SpectrumSetup-C3)
(Teh_Internets)
(SpectrumSetup-42)
(Hoosier)
(PlayBall-5)
(Scibbe)
(MySpectrumWiFi28-2G)
(Kelley 2.4GHz)
(MySpectrumWiFi40-2G)
(MySpectrumWiFi8-2G)
(SpectrumSetup-C5)
(SpectrumSetup-42)
(Fast_Internets)
(SpectrumSetup-1D)
(SpectrumSetup-80)
(SpectrumSetup-80)
(Danger Zone)
(MySpectrumWiFi80-2G)
(Kelley)
(Kelley)
(Ashley-2G)
(SpectrumSetup-90)
(MySpectrumWiFi0d-2G)
(SpectrumSetup-25)
(SpectrumSetup-E8)
(MySpectrumWiFi27-2G)
(HP-Print-F9-ENVY 5530 series)
(MySpectrumWiFi24-2G)
(Kelley 5GHz-Guest)
(the_gate)
(DIRECT-LY-VIZIOTV)
(SpectrumSetup-9D)
(Kelley 5GHz-Guest)
(NETGEAR21)
(SpectrumSetup-27)
(aqqerhome)

1	Active	B0:E4:D5:64:B6:21	Hoosier	85%	85%	-56 dBm	-55 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
2	Active	B0:E4:D5:64:B6:25	Hoosier	88%	91%	-49 dBm	-44 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
3	Active	F0:72:EA:82:CD:72	Hoosier	85%	90%	-56 dBm	-47 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
4	Active	10:0C:6B:EF:16:92	Kelley	31%	38%	-83 dBm	-80 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
5	Dead	74:93:DA:DA:AC:95	SpectrumSetup-97	0%	24%	-100 dBm	-86 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
6	Dead	4C:19:5D:7F:FC:74	SpectrumSetup-6E	0%	18%	-100 dBm	-89 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
7	Active	D8:D7:75:CA:C5:8A	MySpectrumWiFi84-2G	13%	13%	-92 dBm	-92 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
8	Dead	CA:3A:6B:A9:8A:0C		0%	24%	-100 dBm	-86 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
9	Dead	36:21:03:D8:19:AD		0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
10	Active	10:D7:B0:E7:8F:BE	SpectrumSetup-B8	20%	22%	-88 dBm	-87 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
11	Active	B0:39:56:90:C7:D3	PlayBall-2	95%	97%	-38 dBm	-33 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
12	Active	F4:69:42:C7:05:B9	SpectrumSetup-BB	18%	20%	-89 dBm	-88 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
13	Active	FC:12:63:24:73:B9	SpectrumSetup-BB	31%	38%	-83 dBm	-80 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
14	Active	14:7D:05:4D:3D:63	SpectrumSetup-61	40%	43%	-79 dBm	-78 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
15	Active	14:7D:05:9F:81:4F	SpectrumSetup-4D	24%	29%	-86 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
16	Active	30:8D:99:7D:3E:5F	DIRECT-5E-HP ENVY 764...	81%	85%	-62 dBm	-55 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
17	Active	F4:69:42:A4:47:C1	SpectrumSetup-C3	31%	31%	-83 dBm	-83 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
18	Active	20:4E:7F:14:56:B1	Teh_Internets	50%	65%	-76 dBm	-71 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
19	Active	2C:EA:DC:8D:0E:40	SpectrumSetup-42	81%	84%	-63 dBm	-57 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
20	Active	F0:72:EA:82:CD:75	Hoosier	65%	75%	-71 dBm	-67 dBm	149	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
21	Active	B0:39:56:90:C7:D4	PlayBall-5	85%	92%	-56 dBm	-43 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
22	Active	08:7B:12:4D:3B:11	Scibbe	11%	14%	-93 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
23	Active	E8:AD:A6:67:DC:2E	MySpectrumWiFi28-2G	14%	31%	-91 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
24	Active	38:70:0C:49:D5:08	Kelley 2.4GHz	11%	31%	-93 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
25	Active	28:9E:FC:7A:CD:46	MySpectrumWiFi40-2G	18%	24%	-89 dBm	-86 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
26	Active	00:CB:51:4E:82:FE	MySpectrumWiFi8-2G	13%	18%	-92 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
27	Active	74:37:5F:72:F8:C7	SpectrumSetup-C5	29%	40%	-84 dBm	-79 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
28	Active	0E:EA:DC:8D:0E:41	Spectrum Mobile	38%	50%	-80 dBm	-76 dBm	157	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
29	Active	2C:EA:DC:8D:0E:41	SpectrumSetup-42	38%	50%	-80 dBm	-76 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
30	Active	20:4E:7F:14:56:B0	Fast_Internets	26%	35%	-85 dBm	-81 dBm	157	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
31	Active	4C:19:5D:4A:5F:23	SpectrumSetup-1D	11%	18%	-93 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
32	Active	1E:49:5B:CA:2E:83	Spectrum Mobile	16%	22%	-90 dBm	-87 dBm	44	WPA2-Enterprise	CCMP	Infrastructure	N 0.0000000	E 0.000000
33	Active	34:49:5B:CA:2E:87	SpectrumSetup-80	13%	22%	-92 dBm	-87 dBm	44	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
34	Active	34:49:5B:CA:2E:86	SpectrumSetup-80	26%	50%	-85 dBm	-76 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
35	Active	F0:81:75:CB:A9:0E	Danger Zone	18%	20%	-89 dBm	-88 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
36	Active	84:A0:6E:AE:5F:86	MySpectrumWiFi80-2G	16%	26%	-90 dBm	-85 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
37	Active	10:0C:6B:EC:15:EE	Kelley	20%	31%	-88 dBm	-83 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
38	Active	10:0C:6B:EF:16:98	Kelley	40%	50%	-79 dBm	-76 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
39	Dead	28:9E:FC:9F:65:D6	Ashley-2G	0%	14%	-100 dBm	-91 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
40	Dead	F0:81:75:EC:62:96	SpectrumSetup-90	0%	26%	-100 dBm	-85 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
41	Active	54:91:7F:67:3E:08	MySpectrumWiFi0d-2G	16%	20%	-90 dBm	-88 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
42	Active	18:A5:FF:4F:E6:80	TMOBILE-E67E	29%	46%	-84 dBm	-77 dBm	5	OWE	CCMP	Infrastructure	N 0.0000000	E 0.000000
43	Active	5C:FA:25:BF:C9:28	SpectrumSetup-25	16%	16%	-90 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
44	Dead	34:53:D2:36:E1:EE	SpectrumSetup-E8	0%	20%	-100 dBm	-88 dBm	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
45	Active	1C:B0:44:FD:B2:25	MySpectrumWiFi27-2G	24%	31%	-86 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
46	Active	D0:BF:9C:B1:84:F9	HP-Print-F9-ENVY 5530 se...	8%	18%	-95 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
47	Active	B8:EE:0E:DB:8D:2A	MySpectrumWiFi24-2G	22%	22%	-87 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000
48	Active	BA:0C:6B:EF:16:93	Kelley 5 GHz Guest	29%	38%	-84 dBm	-80 dBm	7	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.000000

19. Record the total number of different WLANs that you can detect, along with the number of encryption types. Which type is most common?
WPA2

20. One of the features of Vistumbler is its ability to use audio and text-to-speech information so that the location and strength of WLANs can be detected without the need to constantly monitor the screen. Be sure that the speakers on the laptop computer are turned on.

21. Click Options.

22. Click Speak Signals. Vistumbler will “speak” the percentage of signal strength.

23. Now carry the laptop away from the AP and note the changes. How would this be helpful to an attacker?

It allows an attacker to determine the range and coverage area of the wireless network in real-time. This information helps them identify the network boundaries, weak signal spots, and potential locations where they can remain undetected while still accessing the network. It also assists in finding an optimal position for attempting attacks, such as cracking the network encryption, while maintaining a stable connection to the target AP.

24. Close Vistumbler

Case Project 11-6: Your Personal Wireless Security

Description:

Is the wireless network you own as secure as it should be? Examine your wireless network or that of a friend or neighbor and determine which security model it uses. Next, outline the steps it would take to move it to the next highest level. Estimate how much it would cost and how much time it would take to increase the level. Finally, estimate how long it would take you to replace all the data on your computer and what you might lose if the data were corrupted by an attacker. Would this be motivation to increase your current wireless security model? Write a one-page paper on your work

Introduction:

In today's increasingly connected world, the security of wireless networks is a critical concern for individuals and households. A secure wireless network is essential to protect sensitive information from unauthorized access and cyber threats. This paper examines the current security model of a personal wireless network and explores the steps required to enhance its security. The analysis considers the costs, time involved, and potential consequences of a data breach, ultimately highlighting the importance of proactive measures in maintaining robust network security.

Examining a personal wireless network, I determined that it currently employs the WPA2-Personal (Wi-Fi Protected Access 2) security model. While WPA2 is relatively secure, recent advancements in cyberattacks, such as brute force and dictionary attacks, suggest that moving to a more advanced security model would be prudent. The next highest level of wireless security is WPA3, which provides enhanced encryption algorithms and more robust protections against attacks.

To upgrade to WPA3, several steps would be required. First, the router's firmware needs to be checked to see if it supports WPA3 through an update. If not, purchasing a new router capable of WPA3 is necessary. A reliable, mid-range router supporting WPA3 would cost around $100 to $200, while installation and configuration would take approximately 1-2 hours, probably 2 judging my skill level… including updating passwords for connected devices. This is a small investment considering the increased protection against potential threats.

In the event of a security breach, replacing corrupted data on a computer would be a time-consuming process. Based on the amount of data currently stored, it could take 10 to 12 hours to fully restore everything from backups. The potential loss includes personal documents, photos, and work files that may not have been backed up recently, leading to irreplaceable losses. This scenario highlights the critical importance of improving wireless security and serves as strong motivation to upgrade the network to WPA3. The cost and effort to upgrade are minor compared to the consequences of a successful attack, making the enhancement well worth the time and investment.

Project 13-2: viewing Windows slack and Hidden data

●

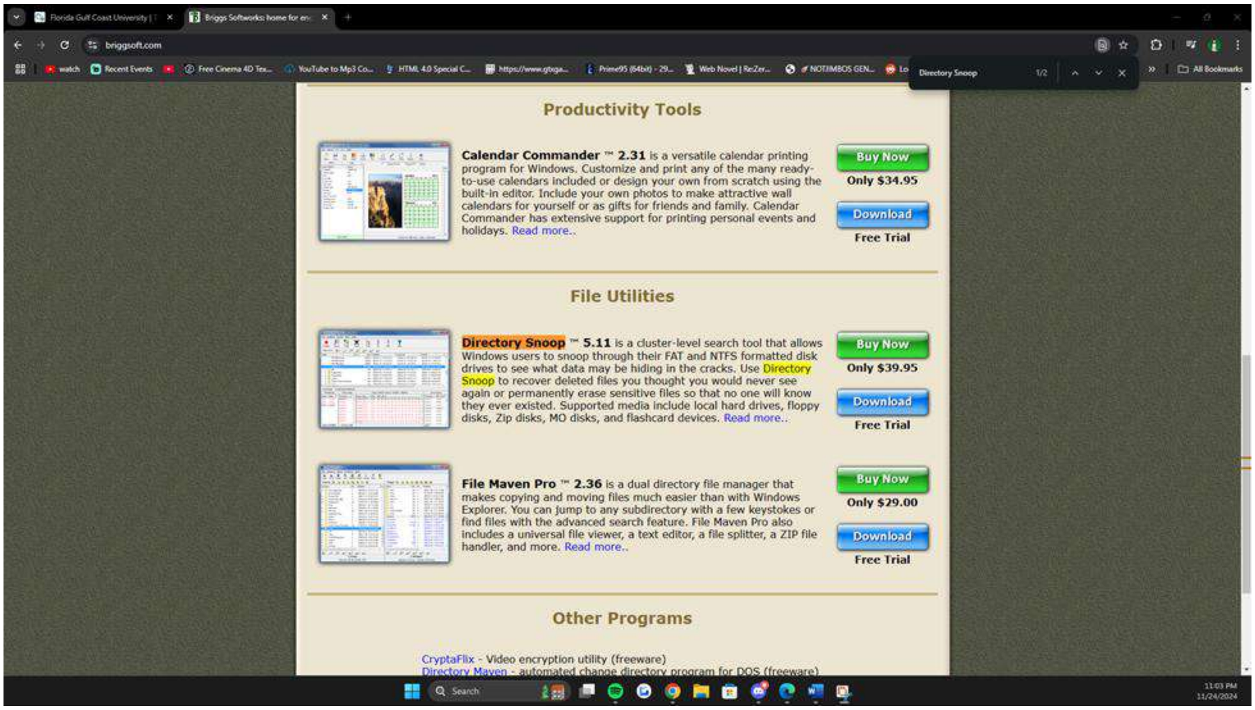
Time required: 20 minutes

Objective: 4.5 Explain the key aspects of digital forensics. Data recovery description: RAM slack, drive slack, and other hidden data can be helpful to a computer forensics investigator. In this project, you download and use a program to search for hidden data.

INTRODUCTION

Digital forensics is the practice of uncovering, analyzing, and preserving electronic data for use in investigations or legal proceedings (Badman & Forrest, 2024). A critical aspect of digital forensics involves identifying and recovering hidden or residual data that may provide vital evidence. This includes analyzing RAM slack (unused space at the end of a file in a memory block), drive slack (unused space between the logical end of a file and the physical end of its storage cluster), and other types of hidden or deleted data.

1. Use your web browser to go to www.briggsoft.com. (The location of content on the Internet may change without warning. If you are no longer able to access the program through the above URL, use a search engine and search for "Directory Snoop.")
2. Scroll down to the current version of directory Snoop and click download above Free Trial.



Productivity Tools

Calendar Commander ™ 2.31 is a versatile calendar printing program for Windows. Customize and print any of the many ready-to-use calendars included or design your own from scratch using the built-in editor. Include your own photos to make attractive wall calendars for yourself or as gifts for friends and family. Calendar Commander has extensive support for printing personal events and holidays. Read more..

Buy Now
Only $34.95
Download
Free Trial

File Utilities

Directory Snoop ™ 5.11 is a cluster-level search tool that allows Windows users to snoop through their FAT and NTFS formatted disk drives to see what data may be hiding in the cracks. Use Directory Snoop to recover deleted files you thought you would never see again or permanently erase sensitive files so that no one will know they ever existed. Supported media include local hard drives, floppy disks, Zip disks, MO disks, and flashcard devices. Read more..

Buy Now
Only $39.95
Download
Free Trial

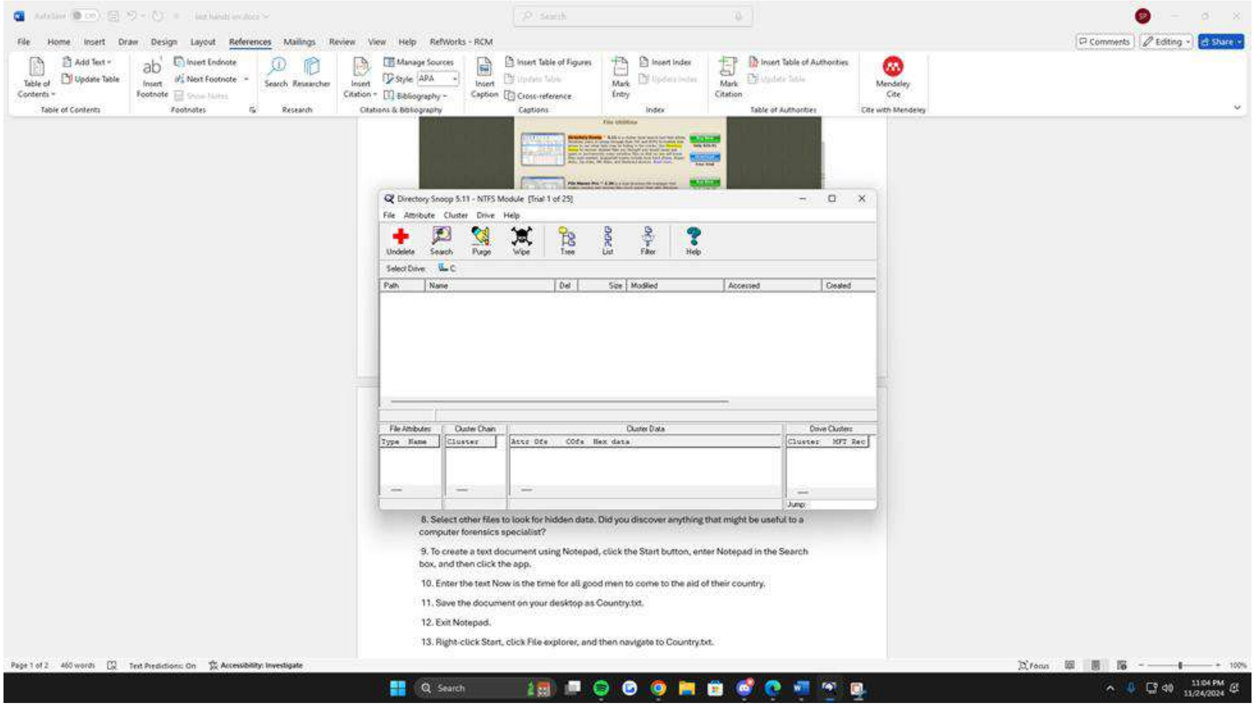
File Maven Pro ™ 2.36 is a dual directory file manager that makes copying and moving files much easier than with Windows Explorer. You can jump to any subdirectory with a few keystrokes or find files with the advanced search feature. File Maven Pro also includes a universal file viewer, a text editor, a file splitter, a ZIP file handler, and more. Read more..

Buy Now
Only $29.00
Download
Free Trial

Other Programs

CryptaFlix - Video encryption utility (freeware)
Directory Maven - automated change directory program for DOS (freeware)

3. Follow the default installation procedures to install Directory Snoop.
4. Launch Directory Snoop.



8. Select other files to look for hidden data. Did you discover anything that might be useful to a computer forensics specialist?

9. To create a text document using Notepad, click the Start button, enter Notepad in the Search box, and then click the app.

10. Enter the text Now is the time for all good men to come to the aid of their country.

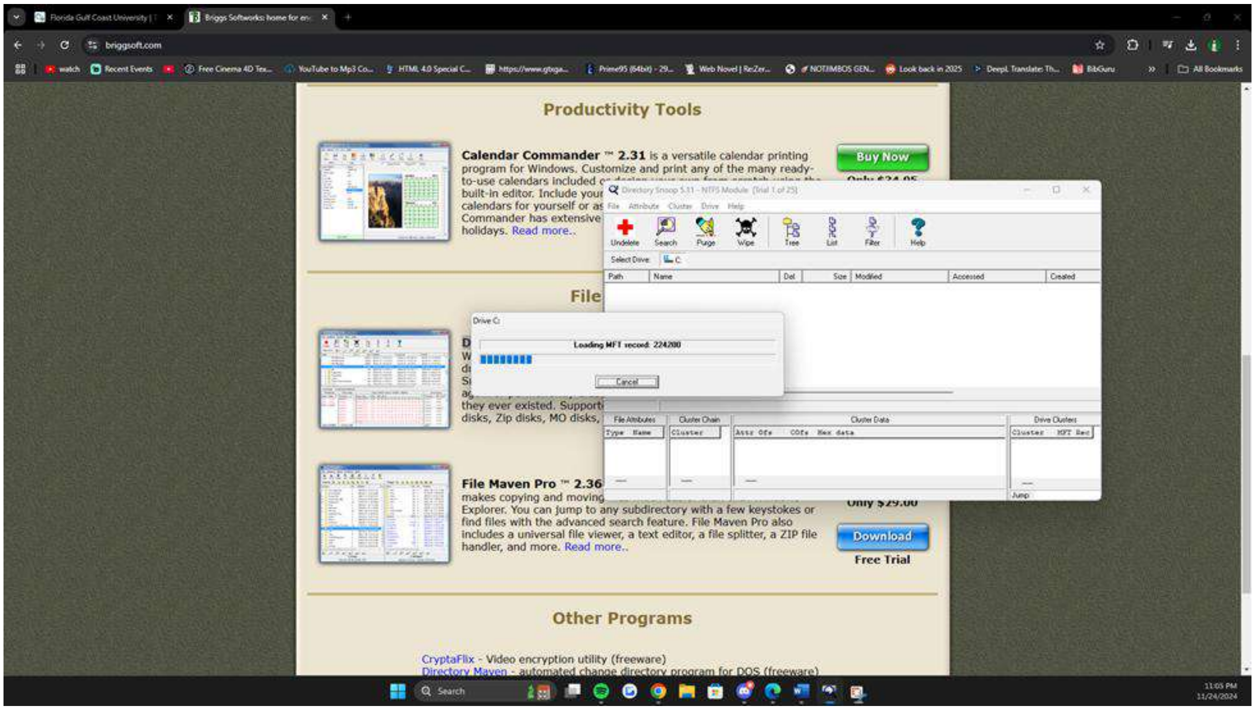
11. Save the document on your desktop as Country.txt.

12. Exit Notepad.

13. Right-click Start, click File explorer, and then navigate to Country.txt.

5. Depending on the filesystem on your computer, click FAT Module or NTFS Module.

6. Under Select Drive, click C:\ or the drive letter of your hard drive. If the RawDisk Driver dialog box appears, click Install driver, click Ok, and then select the appropriate drive again.



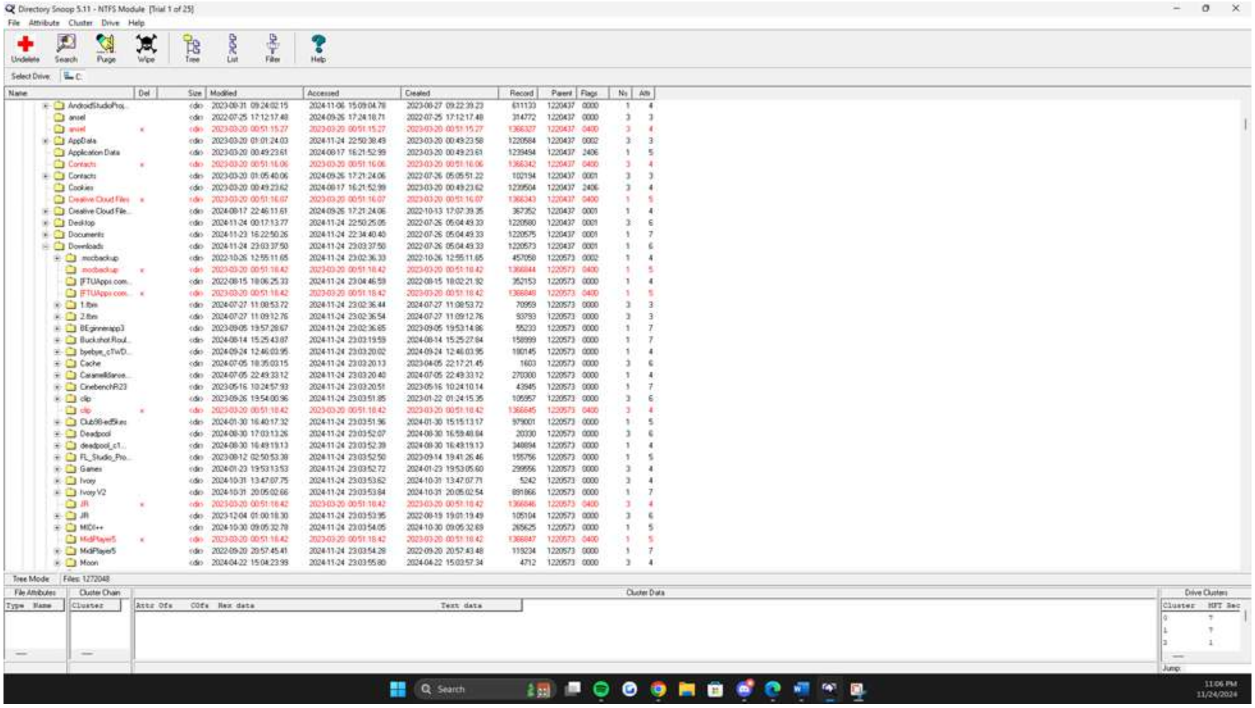
Calendar Commander ™ 2.31 is a versatile calendar printing program for Windows. Customize and print any of the many ready-to-use calendars included o… built-in editor. Include your… calendars for yourself or as… Commander has extensive… holidays. Read more..

File Maven Pro ™ 2.36 makes copying and moving… Explorer. You can jump to any subdirectory with a few keystrokes or find files with the advanced search feature. File Maven Pro also includes a universal file viewer, a text editor, a file splitter, a ZIP file handler, and more. Read more..

Loading MFT record: 224200

CryptaFlix - Video encryption utility (freeware)
Directory Maven - automated change directory program for DOS (freeware)

7. Click to select a file and display its contents, preferably a user-created document (such as a Microsoft Word file).Scroll down under Text data to view the contents that you can read.


Directory Snoop 5.11 - NTFS Module [Trial 1 of 25]
File Attribute Cluster Drive Help
Undelete
Search
Purge
Wipe
Tree
List
Filter
Help
Select Drive: C:
Search
11:06 PM
11/24/2024

Name	Del	Size	Modified	Accessed	Created	Record	Parent	Flags	Ns	Attr
AndroidStudioProj...		<dir>	2023-08-31 09:24:02.15	2024-11-06 15:09:04.78	2023-08-27 09:22:39.23	611133	1220437	0000	1	4
ansel		<dir>	2022-07-25 17:12:17.48	2024-09-26 17:24:18.71	2022-07-25 17:12:17.48	314772	1220437	0000	3	3
ansel	×	<dir>	2023-03-20 00:51:15.27	2023-03-20 00:51:15.27	2023-03-20 00:51:15.27	1366327	1220437	0400	3	4
AppData		<dir>	2023-03-20 01:01:24.03	2024-11-24 22:50:38.49	2023-03-20 00:49:23.58	1220584	1220437	0002	3	3
Application Data		<dir>	2023-03-20 00:49:23.61	2024-08-17 16:21:52.99	2023-03-20 00:49:23.61	1239494	1220437	2406	1	5
Contacts	×	<dir>	2023-03-20 00:51:16.06	2023-03-20 00:51:16.06	2023-03-20 00:51:16.06	1366342	1220437	0400	3	4
Contacts		<dir>	2023-03-20 01:05:40.06	2024-09-26 17:21:24.06	2022-07-26 05:05:51.22	102194	1220437	0001	3	3
Cookies		<dir>	2023-03-20 00:49:23.62	2024-08-17 16:21:52.99	2023-03-20 00:49:23.62	1239504	1220437	2406	3	4
Creative Cloud Files	×	<dir>	2023-03-20 00:51:16.07	2023-03-20 00:51:16.07	2023-03-20 00:51:16.07	1366343	1220437	0400	1	5
Creative Cloud File...		<dir>	2024-08-17 22:46:11.61	2024-09-26 17:21:24.06	2022-10-13 17:07:39.35	367352	1220437	0001	1	4
Desktop		<dir>	2024-11-24 00:17:13.77	2024-11-24 22:50:25.05	2022-07-26 05:04:49.33	1220580	1220437	0001	3	6
Documents		<dir>	2024-11-23 16:22:50.26	2024-11-24 22:34:40.40	2022-07-26 05:04:49.33	1220575	1220437	0001	1	7
Downloads		<dir>	2024-11-24 23:03:37.50	2024-11-24 23:03:37.50	2022-07-26 05:04:49.33	1220573	1220437	0001	1	6
.mocbackup		<dir>	2022-10-26 12:55:11.65	2024-11-24 23:02:36.33	2022-10-26 12:55:11.65	457050	1220573	0002	1	4
.mocbackup	×	<dir>	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	1366844	1220573	0400	1	5
[FTUApps.com...		<dir>	2022-08-15 18:06:25.33	2024-11-24 23:04:46.59	2022-08-15 18:02:21.92	352153	1220573	0000	1	4
[FTUApps.com...	×	<dir>	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	1366848	1220573	0400	1	5
1.fbm		<dir>	2024-07-27 11:08:53.72	2024-11-24 23:02:36.44	2024-07-27 11:08:53.72	70959	1220573	0000	3	3
2.fbm		<dir>	2024-07-27 11:09:12.76	2024-11-24 23:02:36.54	2024-07-27 11:09:12.76	93793	1220573	0000	3	3
BEginnerapp3		<dir>	2023-09-05 19:57:28.67	2024-11-24 23:02:36.65	2023-09-05 19:53:14.86	55233	1220573	0000	1	7
BuckshotRoul...		<dir>	2024-08-14 15:25:43.87	2024-11-24 23:03:19.59	2024-08-14 15:25:27.84	158999	1220573	0000	1	7
byebye_cTWD...		<dir>	2024-09-24 12:46:03.95	2024-11-24 23:03:20.02	2024-09-24 12:46:03.95	180145	1220573	0000	1	4
Cache		<dir>	2024-07-05 18:35:03.15	2024-11-24 23:03:20.13	2023-04-05 22:17:21.45	1603	1220573	0000	3	6
CaramellDance...		<dir>	2024-07-05 22:49:33.12	2024-11-24 23:03:20.40	2024-07-05 22:49:33.12	270300	1220573	0000	1	4
CinebenchR23		<dir>	2023-05-16 10:24:57.93	2024-11-24 23:03:20.51	2023-05-16 10:24:10.14	43945	1220573	0000	1	7
clip		<dir>	2023-09-26 19:54:00.96	2024-11-24 23:03:51.85	2023-01-22 01:24:15.35	105957	1220573	0000	3	6
clip	×	<dir>	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	1366845	1220573	0400	3	4
Club98-ed5kes		<dir>	2024-01-30 16:40:17.32	2024-11-24 23:03:51.96	2024-01-30 15:15:13.17	979001	1220573	0000	1	5
Deadpool		<dir>	2024-08-30 17:03:13.26	2024-11-24 23:03:52.07	2024-08-30 16:59:48.84	20330	1220573	0000	3	6
deadpool_c1...		<dir>	2024-08-30 16:49:19.13	2024-11-24 23:03:52.39	2024-08-30 16:49:19.13	340894	1220573	0000	1	4
FL_Studio_Pro...		<dir>	2023-08-12 02:50:53.38	2024-11-24 23:03:52.50	2023-09-14 19:41:26.46	155756	1220573	0000	1	5
Games		<dir>	2024-01-23 19:53:13.53	2024-11-24 23:03:52.72	2024-01-23 19:53:05.60	299956	1220573	0000	3	4
Ivory		<dir>	2024-10-31 13:47:07.75	2024-11-24 23:03:53.62	2024-10-31 13:47:07.71	5242	1220573	0000	3	4
Ivory V2		<dir>	2024-10-31 20:05:02.66	2024-11-24 23:03:53.84	2024-10-31 20:05:02.54	891866	1220573	0000	1	7
JR	×	<dir>	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	1366846	1220573	0400	3	4
JR		<dir>	2023-12-04 01:00:18.30	2024-11-24 23:03:53.95	2022-08-19 19:01:19.49	105104	1220573	0000	3	6
MIDI++		<dir>	2024-10-30 09:05:32.78	2024-11-24 23:03:54.05	2024-10-30 09:05:32.69	265625	1220573	0000	1	5
MidiPlayer5	×	<dir>	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	2023-03-20 00:51:18.42	1366847	1220573	0400	1	5
MidiPlayer5		<dir>	2022-09-20 20:57:45.41	2024-11-24 23:03:54.28	2022-09-20 20:57:43.48	119234	1220573	0000	1	7
Moon		<dir>	2024-04-22 15:04:23.99	2024-11-24 23:03:55.80	2024-04-22 15:03:57.34	4712	1220573	0000	3	4

Tree Mode Files: 1272048

File Attributes

Type	Name

Cluster Chain

Cluster

Cluster Data

Attr Ofs	COfs	Hex data	Text data

Drive Clusters

Cluster	MFT Sec
0	T
1	T
2	1

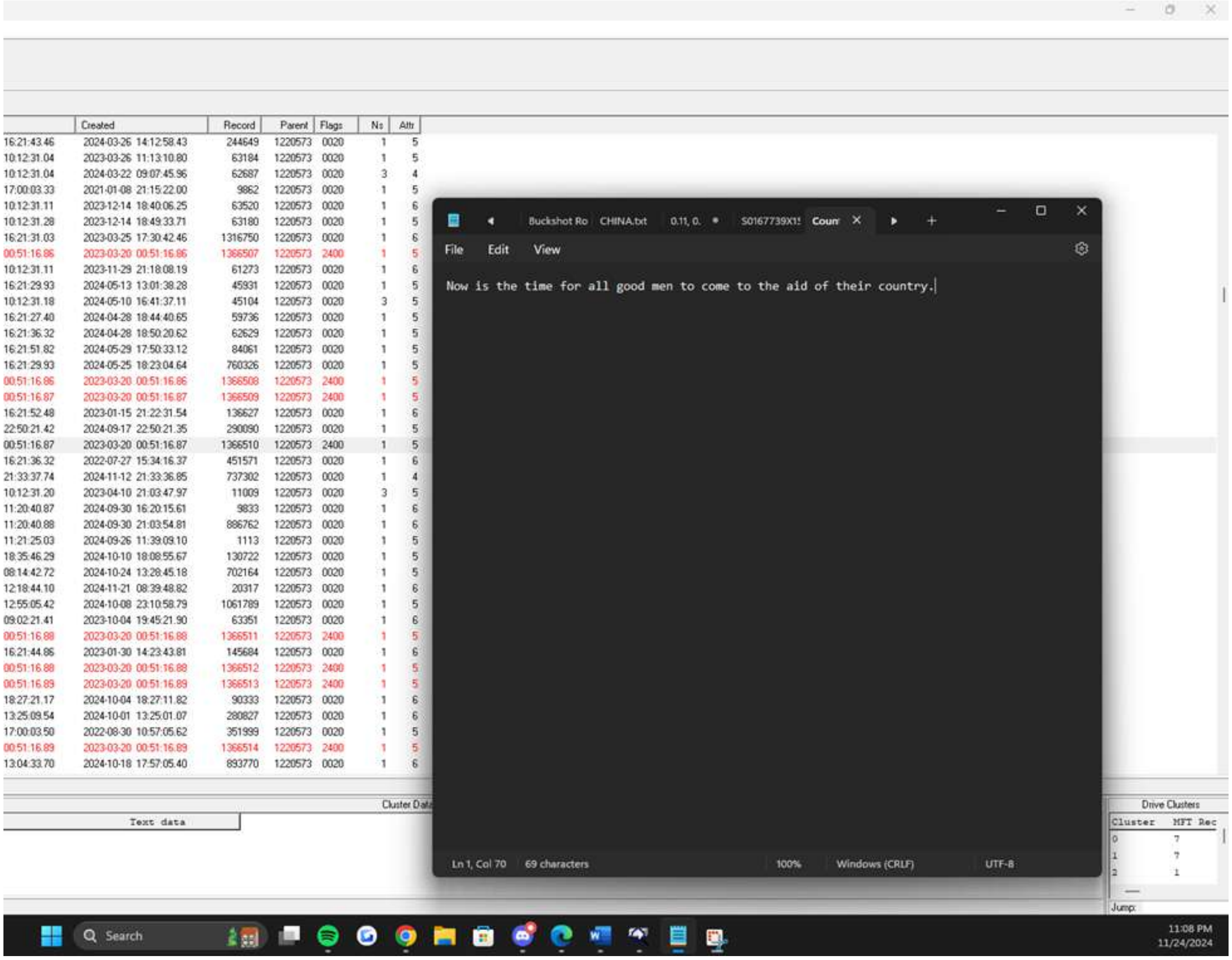
Jump:

8. Select other files to look for hidden data. Did you discover anything that might be useful to a computer forensics specialist?

I am able to view deleted items.

9. To create a text document using Notepad, click the Start button, enter Notepad in the Search box, and then click the app.

10. Enter the text Now is the time for all good men to come to the aid of their country.



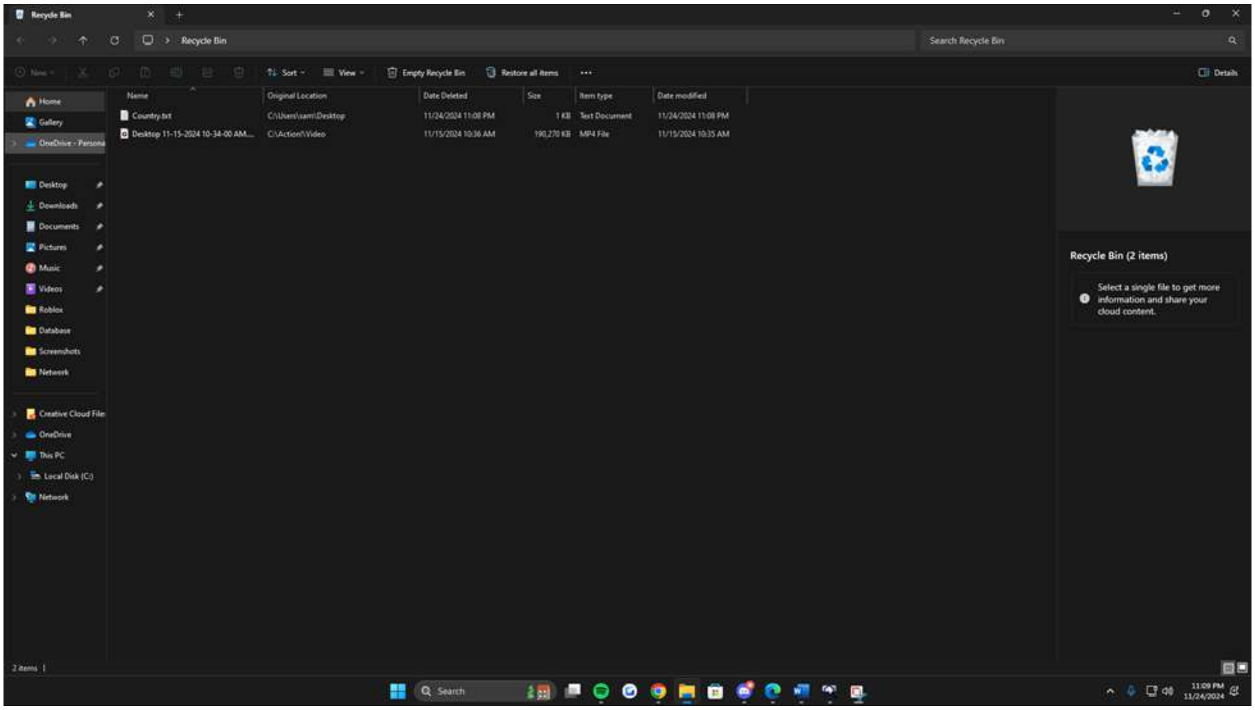
	Created	Record	Parent	Flags	Ns	Attr
16:21:43.46	2024-03-26 14:12:58.43	244649	1220573	0020	1	5
10:12:31.04	2023-03-26 11:13:10.80	63184	1220573	0020	1	5
10:12:31.04	2024-03-22 09:07:45.96	62687	1220573	0020	3	4
17:00:03.33	2021-01-08 21:15:22.00	9862	1220573	0020	1	5
10:12:31.11	2023-12-14 18:40:06.25	63520	1220573	0020	1	6
10:12:31.28	2023-12-14 18:49:33.71	63180	1220573	0020	1	5
16:21:31.03	2023-03-25 17:30:42.46	1316750	1220573	0020	1	6
00:51:16.86	2023-03-20 00:51:16.86	1366507	1220573	2400	1	5
10:12:31.11	2023-11-29 21:18:08.19	61273	1220573	0020	1	6
16:21:29.93	2024-05-13 13:01:38.28	45931	1220573	0020	1	5
10:12:31.18	2024-05-10 16:41:37.11	45104	1220573	0020	3	5
16:21:27.40	2024-04-28 18:44:40.65	59736	1220573	0020	1	5
16:21:36.32	2024-04-28 18:50:20.62	62629	1220573	0020	1	5
16:21:51.82	2024-05-29 17:50:33.12	84061	1220573	0020	1	5
16:21:29.93	2024-05-25 18:23:04.64	760326	1220573	0020	1	5
00:51:16.86	2023-03-20 00:51:16.86	1366508	1220573	2400	1	5
00:51:16.87	2023-03-20 00:51:16.87	1366509	1220573	2400	1	5
16:21:52.48	2023-01-15 21:22:31.54	136627	1220573	0020	1	6
22:50:21.42	2024-09-17 22:50:21.35	290090	1220573	0020	1	5
00:51:16.87	2023-03-20 00:51:16.87	1366510	1220573	2400	1	5
16:21:36.32	2022-07-27 15:34:16.37	451571	1220573	0020	1	6
21:33:37.74	2024-11-12 21:33:36.85	737302	1220573	0020	1	4
10:12:31.20	2023-04-10 21:03:47.97	11009	1220573	0020	3	5
11:20:40.87	2024-09-30 16:20:15.61	9833	1220573	0020	1	6
11:20:40.88	2024-09-30 21:03:54.81	886762	1220573	0020	1	6
11:21:25.03	2024-09-26 11:39:09.10	1113	1220573	0020	1	5
18:35:46.29	2024-10-10 18:08:55.67	130722	1220573	0020	1	5
08:14:42.72	2024-10-24 13:28:45.18	702164	1220573	0020	1	5
12:18:44.10	2024-11-21 08:39:48.82	20317	1220573	0020	1	6
12:55:05.42	2024-10-08 23:10:58.79	1061789	1220573	0020	1	5
09:02:21.41	2023-10-04 19:45:21.90	63351	1220573	0020	1	6
00:51:16.88	2023-03-20 00:51:16.88	1366511	1220573	2400	1	5
16:21:44.86	2023-01-30 14:23:43.81	145684	1220573	0020	1	6
00:51:16.88	2023-03-20 00:51:16.88	1366512	1220573	2400	1	5
00:51:16.89	2023-03-20 00:51:16.89	1366513	1220573	2400	1	5
18:27:21.17	2024-10-04 18:27:11.82	90333	1220573	0020	1	6
13:25:09.54	2024-10-01 13:25:01.07	280827	1220573	0020	1	6
17:00:03.50	2022-08-30 10:57:05.62	351999	1220573	0020	1	5
00:51:16.89	2023-03-20 00:51:16.89	1366514	1220573	2400	1	5
13:04:33.70	2024-10-18 17:57:05.40	893770	1220573	0020	1	6

```
Now is the time for all good men to come to the aid of their country.
```

Ln 1, Col 70 | 69 characters | 100% | Windows (CRLF) | UTF-8

Cluster	MFT Rec
0	7
1	7
2	1

11. Save the document on your desktop as Country.txt.
12. Exit Notepad.
13. Right-click Start, click File explorer, and then navigate to Country.txt.
14. Right-click Country.txt and then click delete to delete the file.



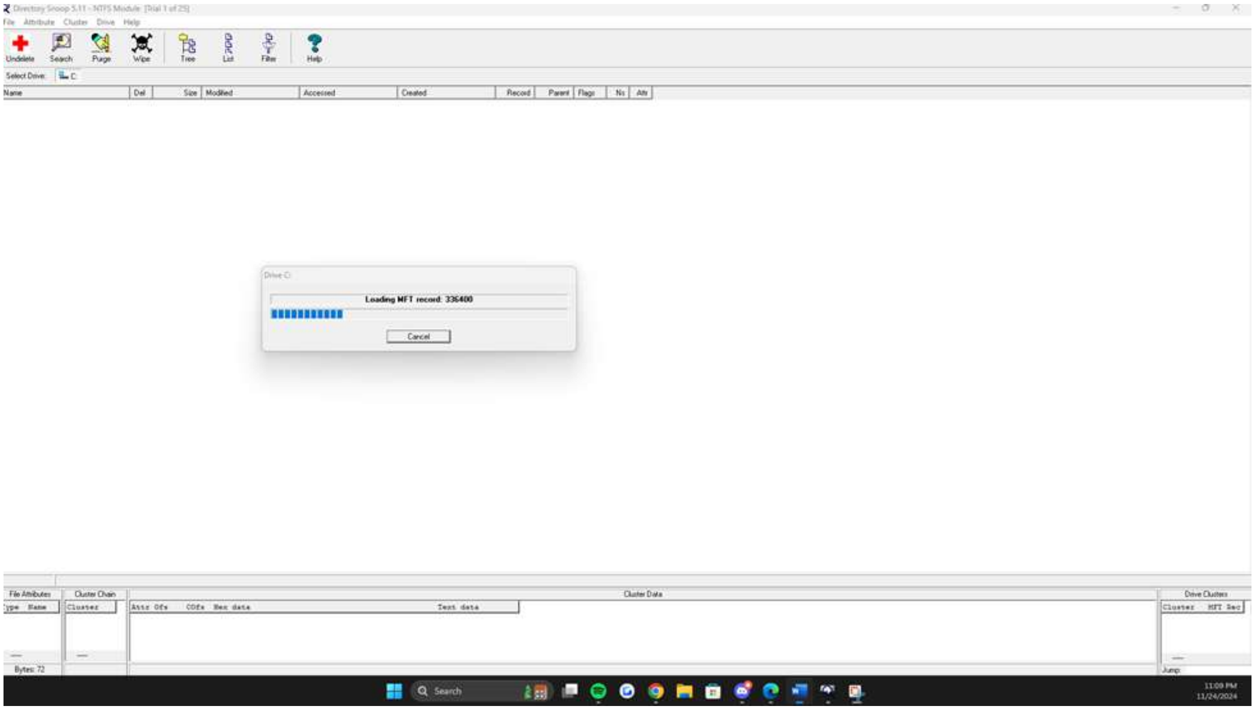
Name	Original Location	Date Deleted	Size	Item type	Date modified
Country.txt	C:\Users\sam\Desktop	11/24/2024 11:08 PM	1 KB	Text Document	11/24/2024 11:08 PM
Desktop 11-15-2024 10-34-00 AM...	C:\Action!\Video	11/15/2024 10:36 AM	190,270 KB	MP4 File	11/15/2024 10:35 AM

Recycle Bin (2 items)

Select a single file to get more information and share your cloud content.

15. Search for information contained in the file you just deleted. Return to directory Snoop, click the top-

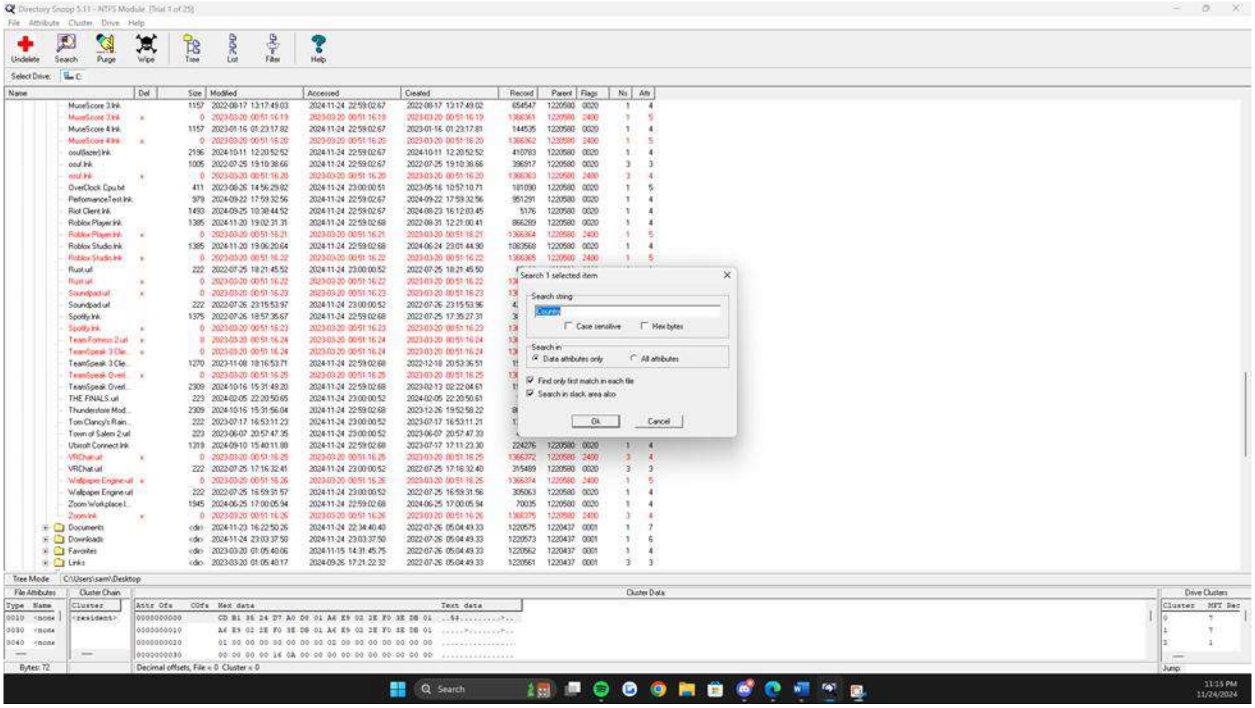
level node for the C:\ drive, and then click the Search icon.


Directory Snoop 5.11 - NTFS Module [Trial 1 of 25]
File Attribute Cluster Drive Help
Undelete
Search
Purge
Wipe
Tree
List
Filter
Help
Select Drive: C:
Name Del Size Modified Accessed Created Record Parent Flags Nx Attr
File Attributes
Cluster Chain
Cluster Data
Drive Clusters
Type Name
Cluster
Attr Ofs COfs Hex data Text data
Cluster MFT Rec
Bytes: 72
Jump:
Search
11:09 PM
11/24/2024

Drive C:

Loading MFT record: 336400

16. Click Files.
17. Enter country as the item that you are searching for.
18. Click Search in slack area also.


Directory Snoop 5.11 - NTFS Module [Trial 1 of 25]
File Attribute Cluster Drive Help
Undelete
Search
Purge
Wipe
Tree
List
Filter
Help
Select Drive: C:
Search
11:15 PM
11/24/2024

Name	Del	Size	Modified	Accessed	Created	Record	Parent	Flags	Nx	Attr
MuseScore 3.lnk		1157	2022-08-17 13:17:49.03	2024-11-24 22:59:02.67	2022-08-17 13:17:49.02	654547	1220580	0020	1	4
MuseScore 3.lnk	x	0	2023-03-20 00:51:16.19	2023-03-20 00:51:16.19	2023-03-20 00:51:16.19	1366361	1220580	2400	1	5
MuseScore 4.lnk		1157	2023-01-16 01:23:17.82	2024-11-24 22:59:02.67	2023-01-16 01:23:17.81	144535	1220580	0020	1	4
MuseScore 4.lnk	x	0	2023-03-20 00:51:16.20	2023-03-20 00:51:16.20	2023-03-20 00:51:16.20	1366362	1220580	2400	1	5
osu!(lazer).lnk		2196	2024-10-11 12:20:52.52	2024-11-24 22:59:02.67	2024-10-11 12:20:52.52	410783	1220580	0020	1	4
osu!.lnk		1005	2022-07-25 19:10:38.66	2024-11-24 22:59:02.67	2022-07-25 19:10:38.66	396917	1220580	0020	3	3
osu!.lnk	x	0	2023-03-20 00:51:16.20	2023-03-20 00:51:16.20	2023-03-20 00:51:16.20	1366363	1220580	2400	3	4
OverClock Cpu.txt		411	2023-08-26 14:56:29.82	2024-11-24 23:00:00.51	2023-05-16 10:57:10.71	181090	1220580	0020	1	5
PerformanceTest.lnk		979	2024-09-22 17:59:32.56	2024-11-24 22:59:02.67	2024-09-22 17:59:32.56	951291	1220580	0020	1	4
Riot Client.lnk		1493	2024-09-25 10:38:44.52	2024-11-24 22:59:02.67	2024-08-23 16:12:03.45	5176	1220580	0020	1	4
Roblox Player.lnk		1385	2024-11-20 19:02:31.31	2024-11-24 22:59:02.68	2022-08-31 12:21:00.41	866289	1220580	0020	1	4
Roblox Player.lnk	x	0	2023-03-20 00:51:16.21	2023-03-20 00:51:16.21	2023-03-20 00:51:16.21	1366364	1220580	2400	1	5
Roblox Studio.lnk		1385	2024-11-20 19:06:20.64	2024-11-24 22:59:02.68	2024-06-24 23:01:44.90	1083568	1220580	0020	1	4
Roblox Studio.lnk	x	0	2023-03-20 00:51:16.22	2023-03-20 00:51:16.22	2023-03-20 00:51:16.22	1366365	1220580	2400	1	5
Rust.url		222	2022-07-25 18:21:45.52	2024-11-24 23:00:00.52	2022-07-25 18:21:45.50	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Rust.url	x	0	2023-03-20 00:51:16.22	2023-03-20 00:51:16.22	2023-03-20 00:51:16.22	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Soundpad.url	x	0	2023-03-20 00:51:16.23	2023-03-20 00:51:16.23	2023-03-20 00:51:16.23	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Soundpad.url		222	2022-07-26 23:15:53.97	2024-11-24 23:00:00.52	2022-07-26 23:15:53.96	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Spotify.lnk		1375	2022-07-26 18:57:36.67	2024-11-24 22:59:02.68	2022-07-25 17:35:27.31	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Spotify.lnk	x	0	2023-03-20 00:51:16.23	2023-03-20 00:51:16.23	2023-03-20 00:51:16.23	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Team Fortress 2.url	x	0	2023-03-20 00:51:16.24	2023-03-20 00:51:16.24	2023-03-20 00:51:16.24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
TeamSpeak 3 Clie...	x	0	2023-03-20 00:51:16.24	2023-03-20 00:51:16.24	2023-03-20 00:51:16.24	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
TeamSpeak 3 Clie...		1270	2023-11-08 18:16:53.71	2024-11-24 22:59:02.68	2022-12-18 20:53:36.51	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
TeamSpeak Overl...	x	0	2023-03-20 00:51:16.25	2023-03-20 00:51:16.25	2023-03-20 00:51:16.25	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
TeamSpeak Overl...		2309	2024-10-16 15:31:49.20	2024-11-24 22:59:02.68	2023-02-13 02:22:04.61	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
THE FINALS.url		223	2024-02-05 22:20:50.65	2024-11-24 23:00:00.52	2024-02-05 22:20:50.61	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Thunderstore Mod...		2309	2024-10-16 15:31:56.04	2024-11-24 22:59:02.68	2023-12-26 19:52:58.22	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Tom Clancy's Rain...		222	2023-07-17 16:53:11.23	2024-11-24 23:00:00.52	2023-07-17 16:53:11.21	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Town of Salem 2.url		223	2023-06-07 20:57:47.35	2024-11-24 23:00:00.52	2023-06-07 20:57:47.33	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Ubisoft Connect.lnk		1319	2024-09-10 15:40:11.88	2024-11-24 22:59:02.68	2023-07-17 17:11:23.30	224276	1220580	0020	1	4
VRChat.url	x	0	2023-03-20 00:51:16.25	2023-03-20 00:51:16.25	2023-03-20 00:51:16.25	1366372	1220580	2400	3	4
VRChat.url		222	2022-07-25 17:16:32.41	2024-11-24 23:00:00.52	2022-07-25 17:16:32.40	315489	1220580	0020	3	3
Wallpaper Engine.url	x	0	2023-03-20 00:51:16.26	2023-03-20 00:51:16.26	2023-03-20 00:51:16.26	1366374	1220580	2400	1	5
Wallpaper Engine.url		222	2022-07-25 16:59:31.57	2024-11-24 23:00:00.52	2022-07-25 16:59:31.56	305063	1220580	0020	1	4
Zoom Workplace.l...		1945	2024-06-25 17:00:05.94	2024-11-24 22:59:02.68	2024-06-25 17:00:05.94	70035	1220580	0020	1	4
Zoom.lnk	x	0	2023-03-20 00:51:16.26	2023-03-20 00:51:16.26	2023-03-20 00:51:16.26	1366375	1220580	2400	3	4
Documents		<dir>	2024-11-23 16:22:50.26	2024-11-24 22:34:40.40	2022-07-26 05:04:49.33	1220575	1220437	0001	1	7
Downloads		<dir>	2024-11-24 23:03:37.50	2024-11-24 23:03:37.50	2022-07-26 05:04:49.33	1220573	1220437	0001	1	6
Favorites		<dir>	2023-03-20 01:05:40.06	2024-11-15 14:31:45.75	2022-07-26 05:04:49.33	1220562	1220437	0001	1	4
Links		<dir>	2023-03-20 01:05:40.17	2024-09-26 17:21:22.32	2022-07-26 05:04:49.33	1220561	1220437	0001	3	3

Search 1 selected item

Search string: Country

☐ Case sensitive ☐ Hex bytes

Search in: ● Data attributes only ○ All attributes

☑ Find only first match in each file

☑ Search in slack area also

Tree Mode: C:\Users\sam\Desktop

Type	Name
0010	<none
0030	<none
0040	<none

Cluster
<resident>

```
Attr Ofs    COfs Hex data                                          Text data
0000000000       CD B1 35 24 D7 A0 D0 01 A6 E9 02 2E F0 3E DB 01   ..5$........?..
0000000010       A6 E9 02 2E F0 3E DB 01 A6 E9 02 2E F0 3E DB 01   .....>......?..
0000000020       01 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00   ................
0000000030       00 00 00 00 14 0A 00 00 00 00 00 00 00 00 00 00   ................
```

Bytes: 72

Decimal offsets, File = 0 Cluster = 0

Cluster	MFT Rec
0	7
1	7
2	1

19. Click Ok. Did the program find this data? Why or why not?

When you delete items, they aren't actually being deleted. It takes multiple disk clears to remove the slack.

20. Close all windows.

Case project 12-1: testing password strength
How strong are your passwords? various online tools can provide information on password strength, but not all feedback is the same. First, assign the numbers 1 through 3 to three passwords that are very similar (but not identical) to passwords you are currently using, and write down the number (not the password) on a piece of paper. Then, enter those passwords into these three online password testing services:

- how secure is My Password (howsecureismypassword.net/)
- Password checker online (password-checker.online-domain-tools.com)
- Password Meter (www.passwordmeter.com/)

Record next to each number the strength of that password as indicated by these three online tools. Then use each online password tester to modify the password by adding more random numbers or letters to increase its strength. How secure are your passwords? Would any of these tools encourage someone to create a stronger password? Which provided the best information? Create a one-paragraph summary of your findings.

1. 1 trillion years, 143 billion years
2. 200 years, 3 years
3. 1 trillion years, 143 billion years

INTRODUCTION
Passwords are the first line of defense against unauthorized access to our sensitive information. A strong password can significantly deter cyberattacks, while a weak one can leave you vulnerable to data breaches (California State University Northridge, n.d.). To assess the strength of your passwords, you can utilize various online tools. It's crucial to understand that not all password strength assessments are created equal. By comparing the feedback from different tools, you can gain a more comprehensive understanding of your password's security.

I would agree that these tools would motivate people to create stronger passwords. I compared my old password (#2) to my new password styles (#1 and #3) and found a significant improvement in security. While my old password could be cracked in a mere 3 years, my new passwords boast an estimated cracking time of billions of years. The second website provided a detailed breakdown of brute force methods, revealing that even with a medium botnet, it would take an astonishing 143 billion years to crack my new passwords. However, it's important to remember that the strength of a password is only one layer of security. If a database containing your password is compromised, attackers can bypass the cracking process entirely, highlighting the need for robust security measures beyond strong passwords such as two-factor authentication.

References

Badman, A., & Forrest, A. (2024, February 24). *What is digital forensics?* Retrieved from IBM: https://www.ibm.com/topics/digital-forensics

California State University Northridge. (n.d.). *Week 1 - Use Strong Passwords & a Password Manager*. Retrieved from CSUN: https://w2.csun.edu/it/information-security/2024-cybersecurity-awareness-month/week-1-use-strong-passwords-password

IEEE. (n.d.). *WPA3 standard overview*. IEEE Xplore. https://ieeexplore.ieee.org

Krebs, B. (n.d.). *Wi-Fi security and WPA3*. Krebs on Security. https://krebsonsecurity.com

National Institute of Standards and Technology (NIST). (n.d.). *Wireless security guidelines*. NIST. https://csrc.nist.gov/publications/detail/sp/800-153/final

Netgear. (n.d.). *Support*. Netgear. https://www.netgear.com/support/

Wi-Fi Alliance. (n.d.). *WPA3 security*. Wi-Fi Alliance. https://www.wi-fi.org/discover-wi-fi/security