Introduction to Information Security & Forensics

Muhammad Harris, BCS203193

Capital University of Science & Technology

Assignment 01

Submitted to Sir *Amir Zaheer*

Introduction to Information Security & Forensics

Question 1

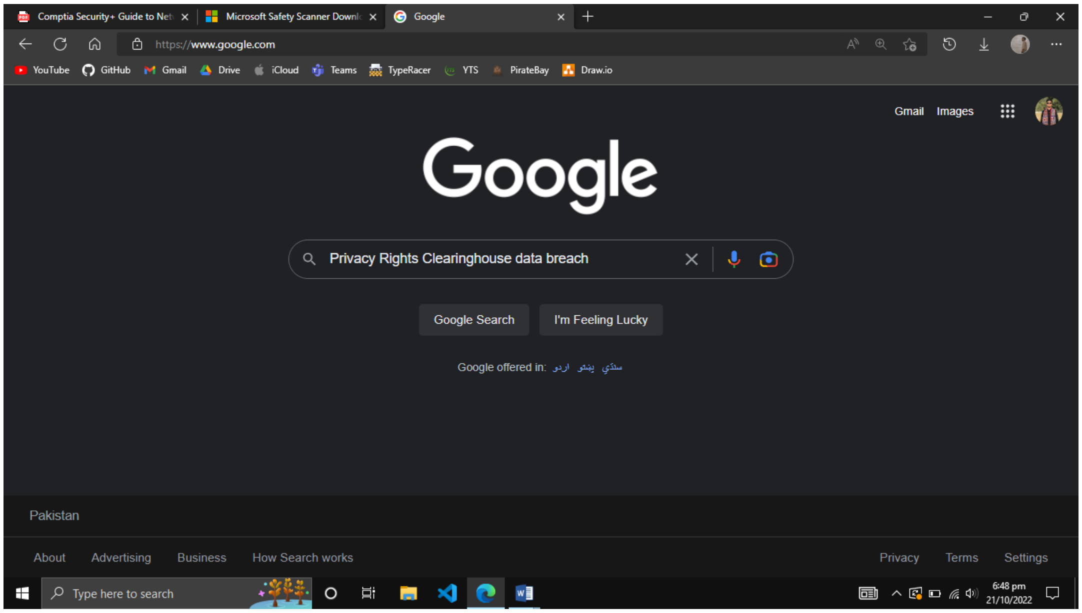
Hands on Projects: Different Hands-on projects are mentioned in the end of chapter 01 of recommended book (Comptia Security + Guide to Network Security Fundamentals). Complete following projects. Take screenshot of each step and submit in assignment.

- *Project 1-1: Examining Data Breaches—Textual*
- *Project 1-3: Scanning for Malware Using the Microsoft Safety Scanner*
- *Project 1-5: Creating a Virtual Machine of Windows 10 for Security Testing*

Project 1-1: ***Examining data breaches***

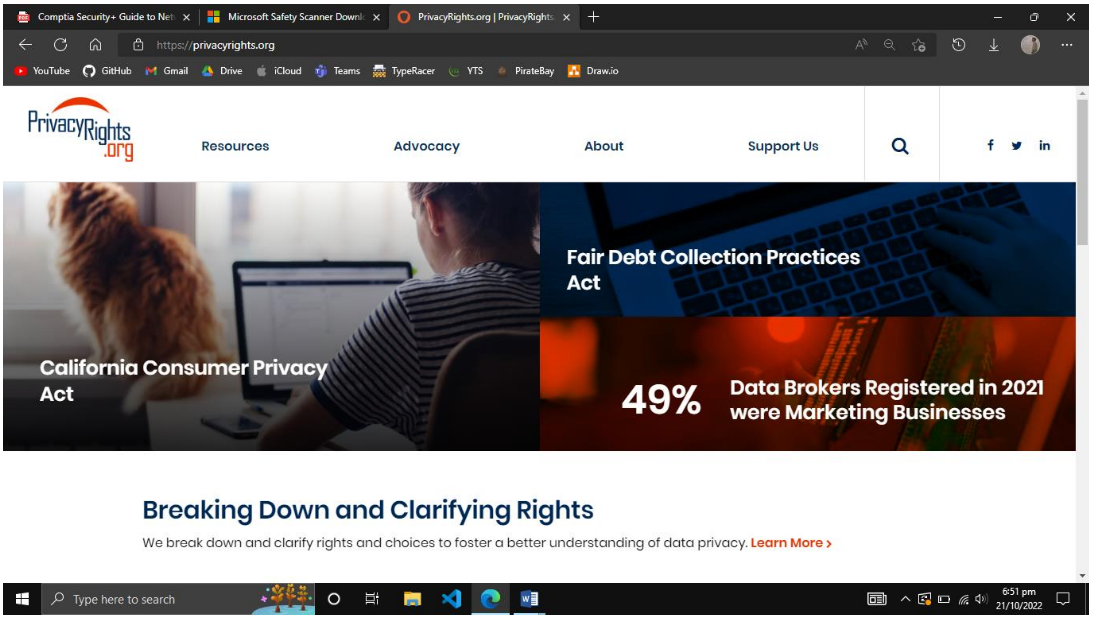
The Privacy Rights Clearinghouse (PRC) is a nonprofit organization whose goals are to raise consumers' awareness of how technology affects personal privacy and empower consumers to take action to control their own personal information. The PRC maintains a searchable database of security breaches that impact consumer's privacy. In this project, you gather information from the PRC website. Open a web browser and enter the URL www.privacyrights.org (if you are no longer able to access the site through the web address, use a search engine to search for "Privacy Rights Clearinghouse data breach."

1. Open a web browser and enter the URL www.privacyrights.org (if you are no longer able to access the site through the web address, use a search engine to search for “Privacy Rights Clearinghouse data breach.”



Privacy Rights Clearinghouse data breach

2. First spend time reading about the PRC by clicking LEARN MORE.



Fair Debt Collection Practices Act

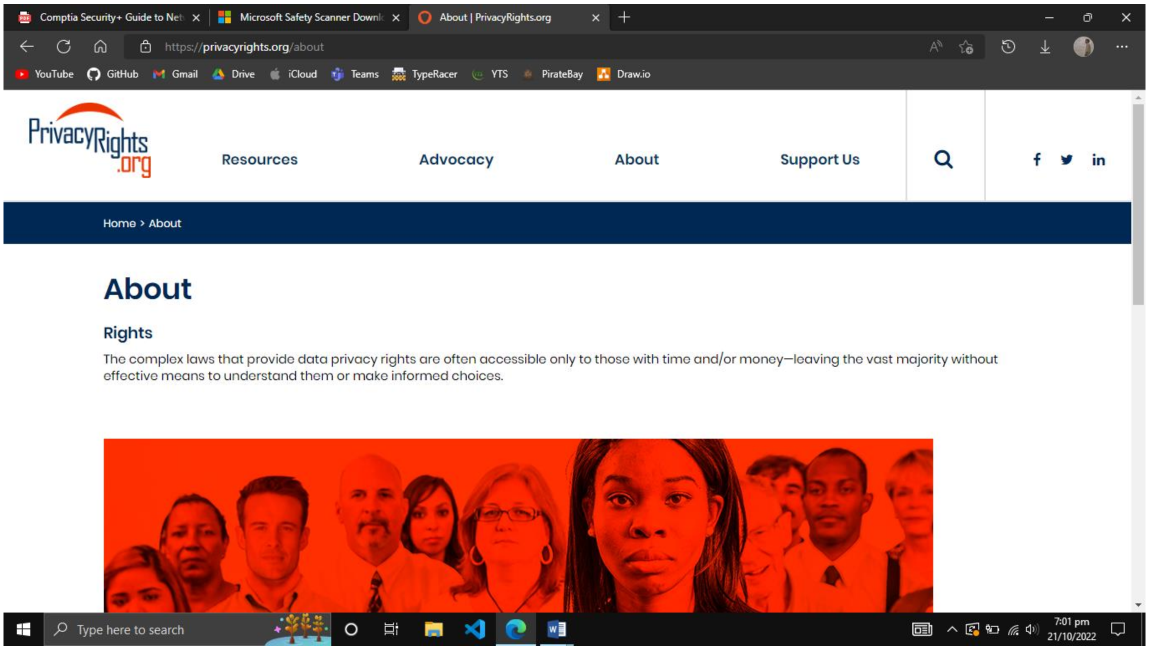
California Consumer Privacy Act

49% Data Brokers Registered in 2021 were Marketing Businesses

Breaking Down and Clarifying Rights

We break down and clarify rights and choices to foster a better understanding of data privacy. Learn More ›

3. Click Data Breaches at the top of the page.

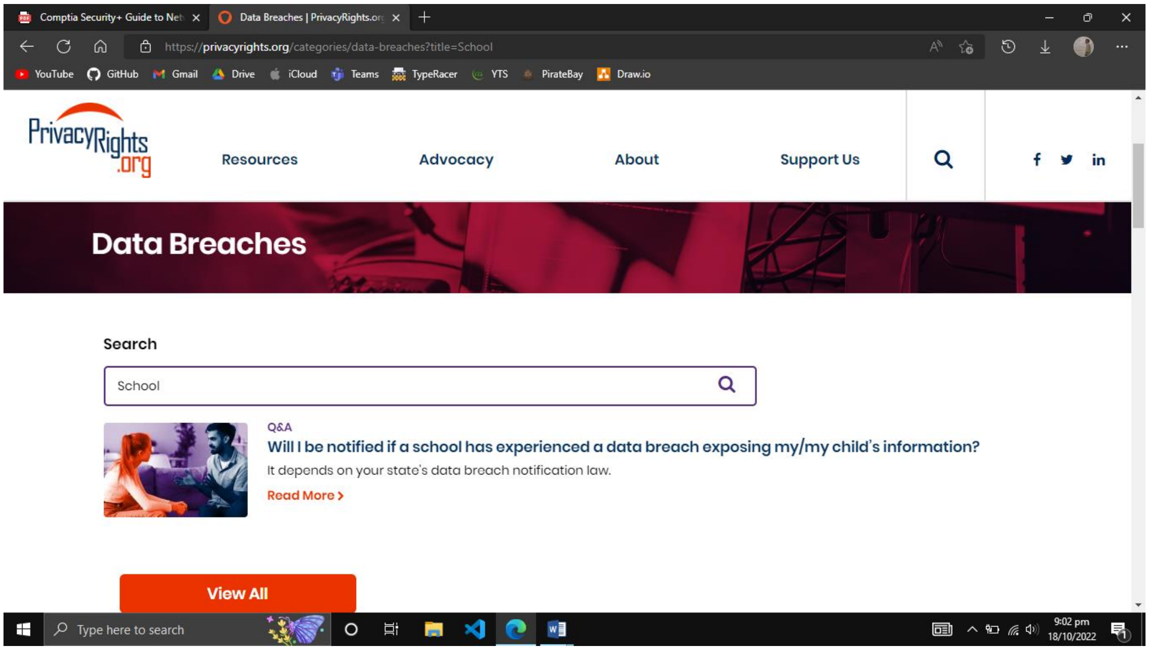


About

Rights

The complex laws that provide data privacy rights are often accessible only to those with time and/or money—leaving the vast majority without effective means to understand them or make informed choices.

4. In the search bar enter a school, organization, or business with which you are familiar to determine if it has been the victim of an attack in which your data has been compromised.



Data Breaches

Search

School

Q&A

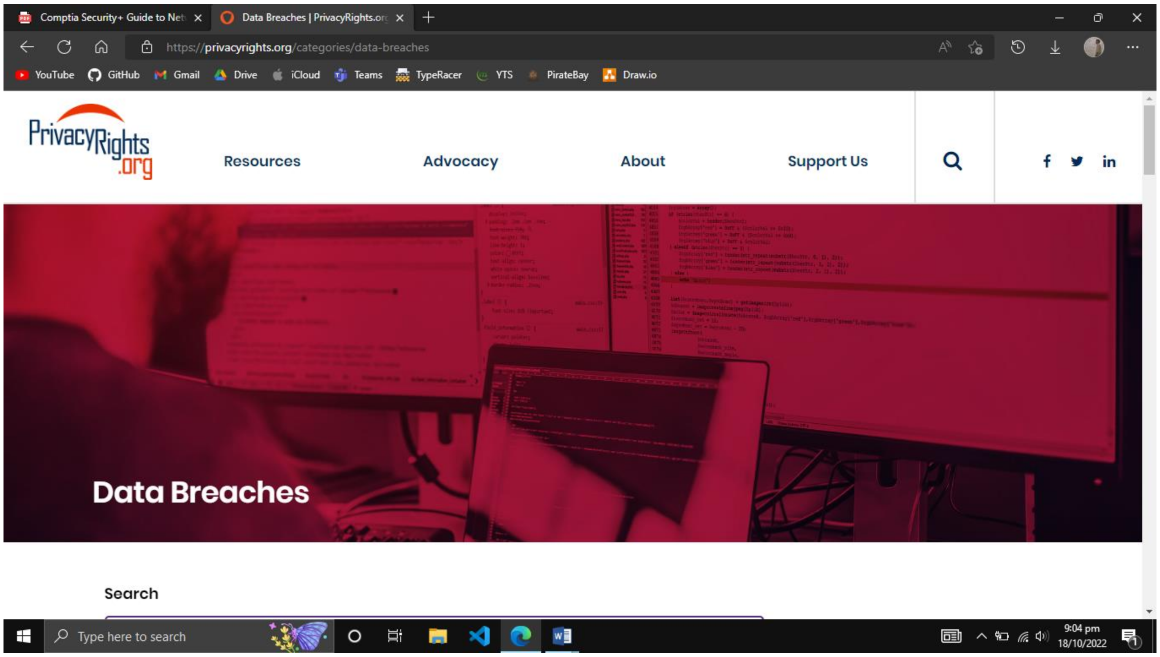
Will I be notified if a school has experienced a data breach exposing my/my child's information?

It depends on your state's data breach notification law.

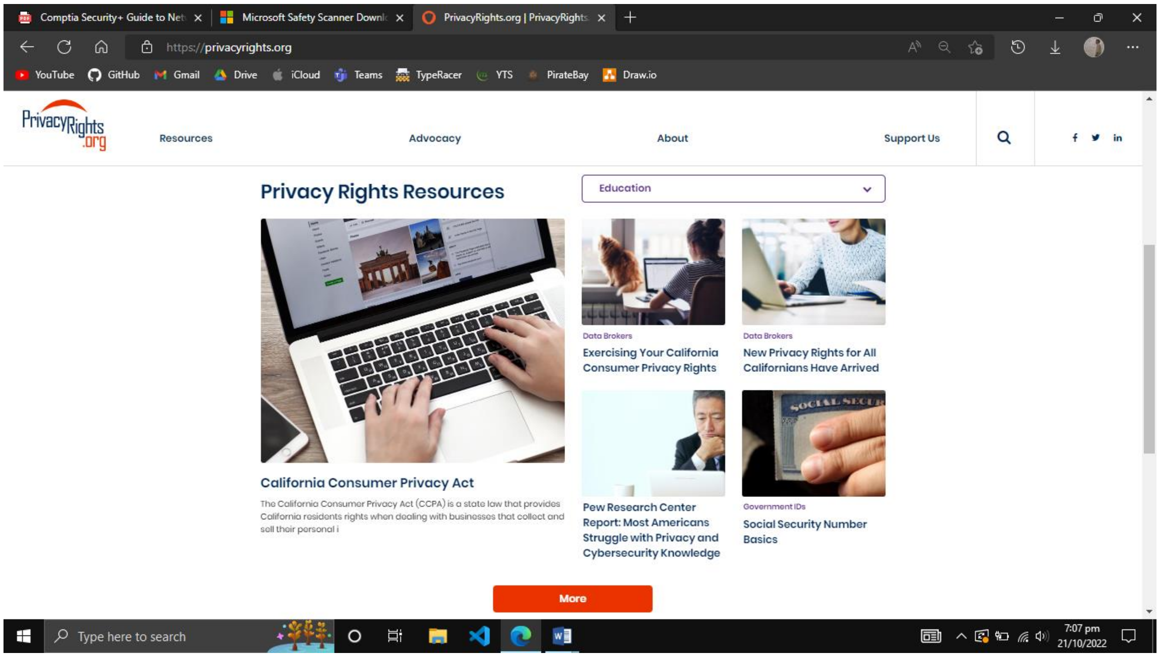
Read More >

View All

5. Click Data Breaches to return to the main Data Breaches page.


Comptia Security+ Guide to Net
Data Breaches | PrivacyRights.or
https://privacyrights.org/categories/data-breaches
YouTube GitHub Gmail Drive iCloud Teams TypeRacer YTS PirateBay Draw.io
PrivacyRights.org
Resources
Advocacy
About
Support Us
Data Breaches
Search
Type here to search
9:04 pm
18/10/2022

6. Now create a customized list of the data that will only list data breaches of educational institutions. Under Select organization type(s), check only EDU-Educational Institutions.


Comptia Security+ Guide to Net
Microsoft Safety Scanner Downl
PrivacyRights.org | PrivacyRights
https://privacyrights.org
YouTube GitHub Gmail Drive iCloud Teams TypeRacer YTS PirateBay Draw.io
PrivacyRights.org
Resources
Advocacy
About
Support Us
Education
More
Type here to search
7:07 pm
21/10/2022

Privacy Rights Resources

Data Brokers
Exercising Your California Consumer Privacy Rights

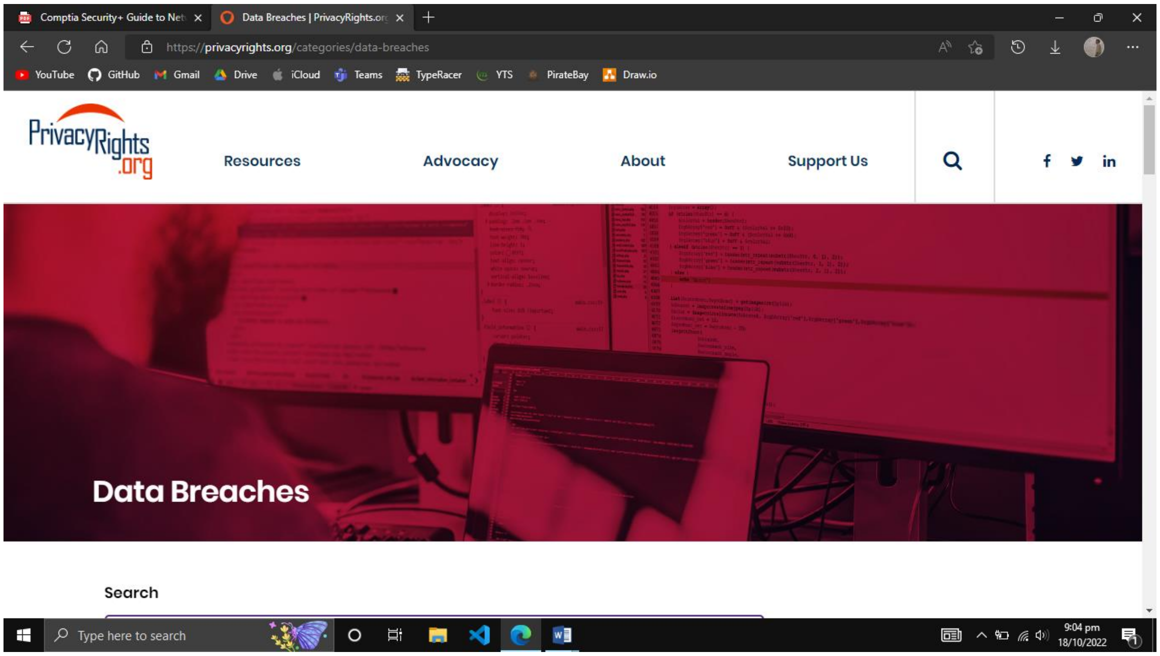
Data Brokers
New Privacy Rights for All Californians Have Arrived

California Consumer Privacy Act
The California Consumer Privacy Act (CCPA) is a state law that provides California residents rights when dealing with businesses that collect and sell their personal i

Pew Research Center Report: Most Americans Struggle with Privacy and Cybersecurity Knowledge

Government IDs
Social Security Number Basics

7. Click Search Data Breaches.

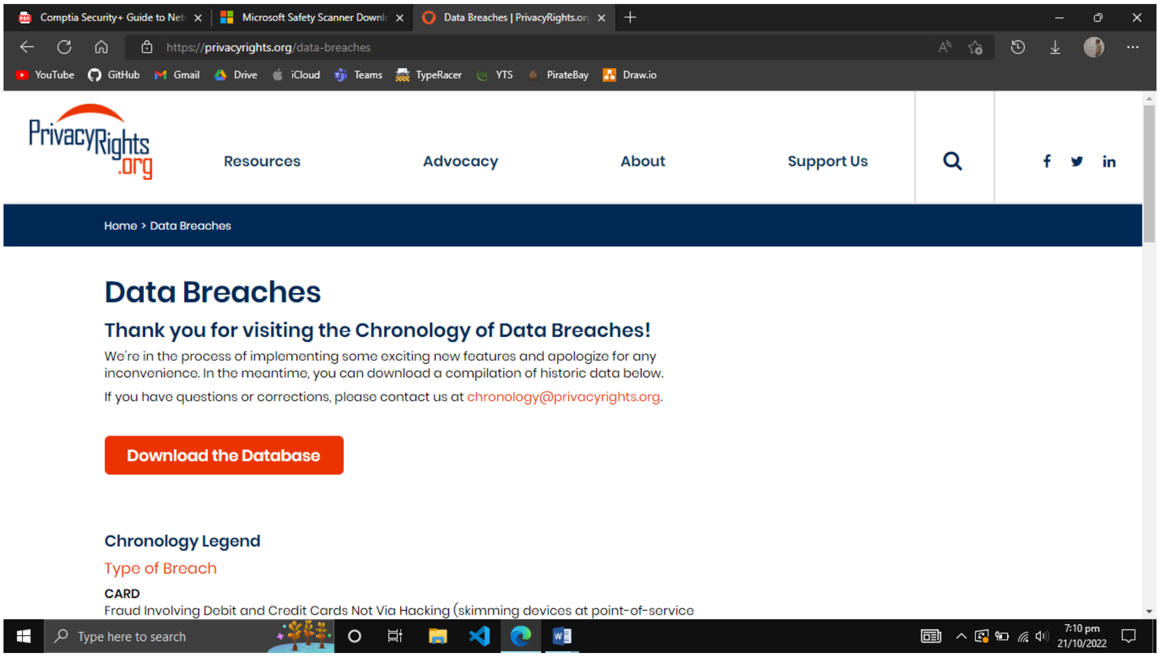


Data Breaches

Search

8. Read the Breach Subtotal information. How many breaches that were made public pertain to educational institutions? How many total records were stolen?

There were total 9016 breaches out of which 843 were on Educational institutes. Number of records stole were 131144394. (<u>Data provided in Database file</u>)



Data Breaches

Thank you for visiting the Chronology of Data Breaches!

We're in the process of implementing some exciting new features and apologize for any inconvenience. In the meantime, you can download a compilation of historic data below.

If you have questions or corrections, please contact us at chronology@privacyrights.org.

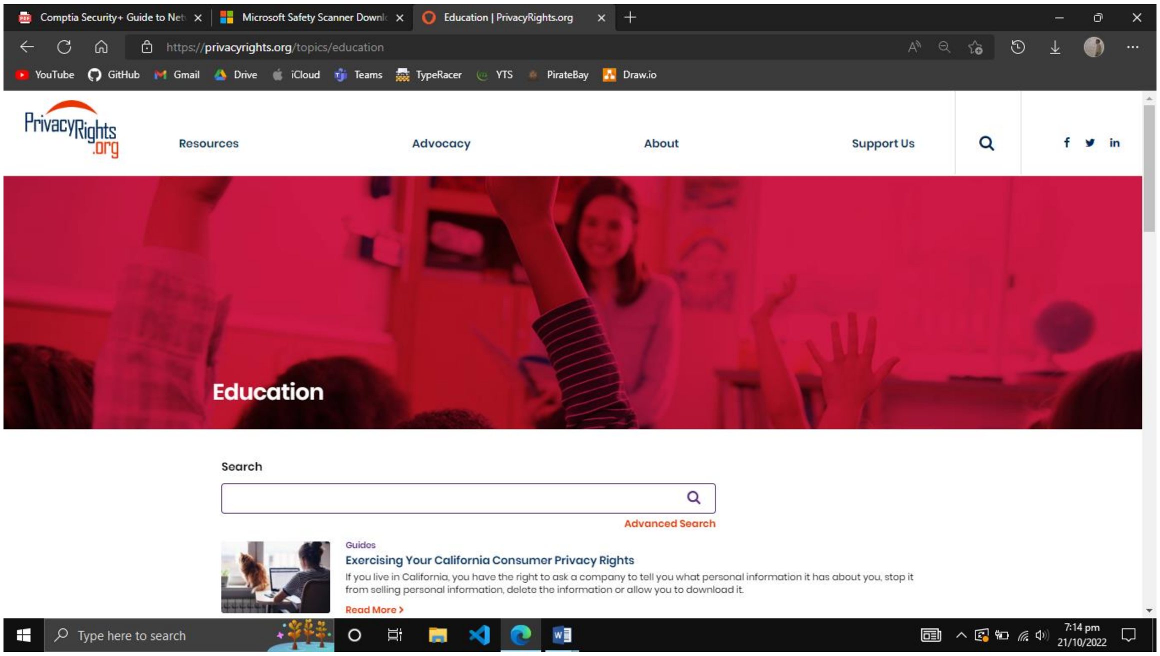
Chronology Legend

Type of Breach

CARD

Fraud Involving Debit and Credit Cards Not Via Hacking (skimming devices at point-of-service

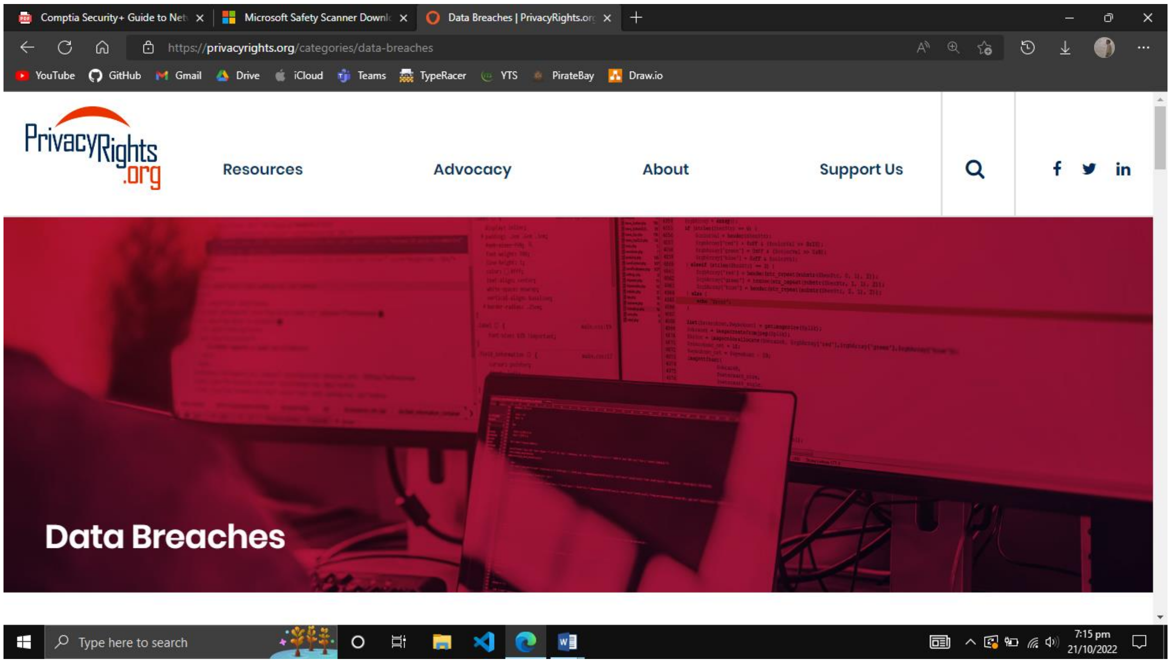
9. Scroll down and observe the breaches for educational institutions.



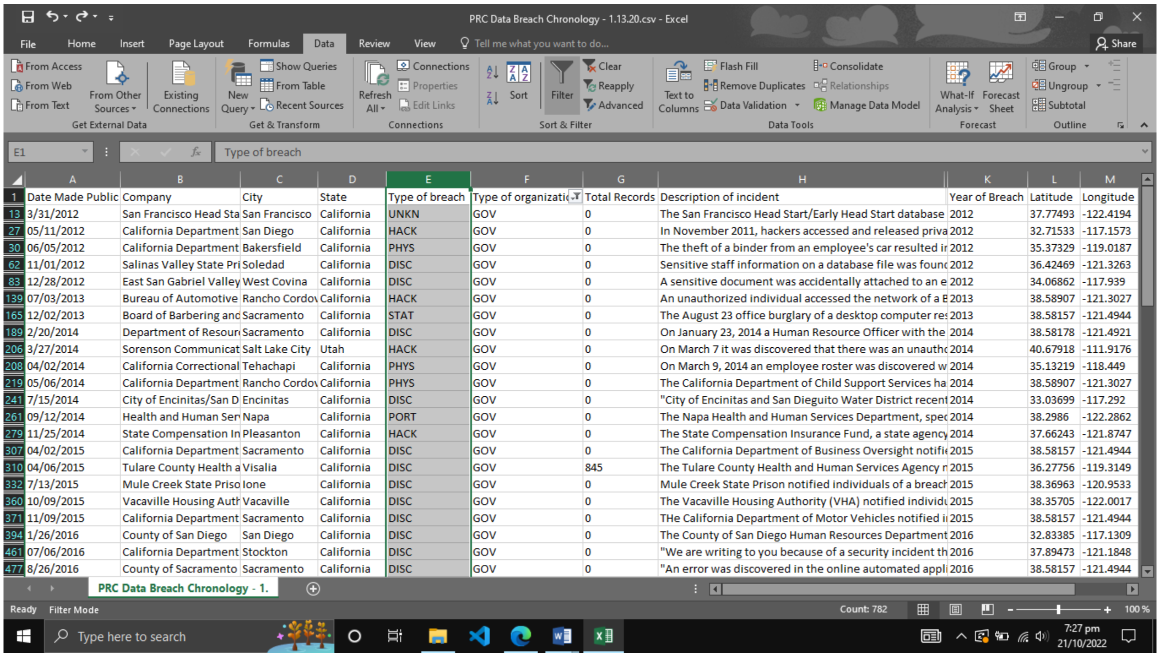
Exercising Your California Consumer Privacy Rights

If you live in California, you have the right to ask a company to tell you what personal information it has about you, stop it from selling personal information, delete the information or allow you to download it.

10. Scroll back to the top of the page. Click New Data Breach Search.



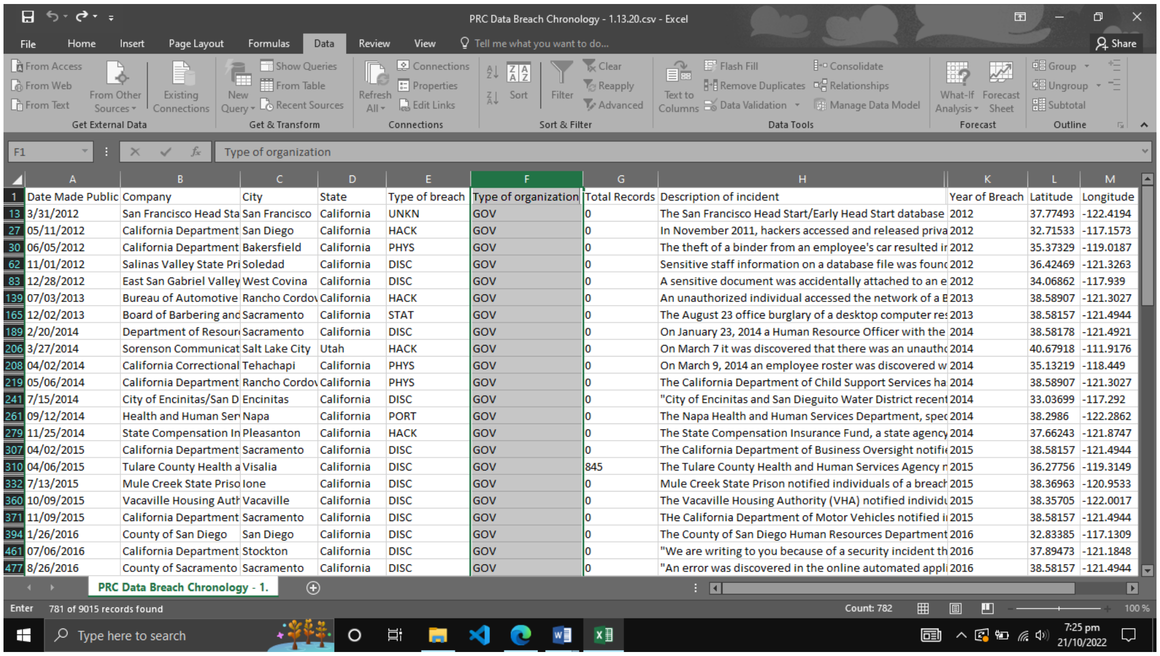
11. Now search for breaches that were a result of lost, discarded, or stolen equipment that belonged to the government and military. Under choose the type of breaches to display, check Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.



E1 — Type of breach

	A	B	C	D	E	F	G	H	K	L	M
1	Date Made Public	Company	City	State	Type of breach	Type of organizatio	Total Records	Description of incident	Year of Breach	Latitude	Longitude
13	3/31/2012	San Francisco Head Sta	San Francisco	California	UNKN	GOV	0	The San Francisco Head Start/Early Head Start database	2012	37.77493	-122.4194
27	05/11/2012	California Department	San Diego	California	HACK	GOV	0	In November 2011, hackers accessed and released priva	2012	32.71533	-117.1573
30	06/05/2012	California Department	Bakersfield	California	PHYS	GOV	0	The theft of a binder from an employee's car resulted ir	2012	35.37329	-119.0187
62	11/01/2012	Salinas Valley State Pri	Soledad	California	DISC	GOV	0	Sensitive staff information on a database file was founc	2012	36.42469	-121.3263
83	12/28/2012	East San Gabriel Valley	West Covina	California	DISC	GOV	0	A sensitive document was accidentally attached to an e	2012	34.06862	-117.939
139	07/03/2013	Bureau of Automotive	Rancho Cordov	California	HACK	GOV	0	An unauthorized individual accessed the network of a E	2013	38.58907	-121.3027
165	12/02/2013	Board of Barbering and	Sacramento	California	STAT	GOV	0	The August 23 office burglary of a desktop computer re:	2013	38.58157	-121.4944
189	2/20/2014	Department of Resour	Sacramento	California	DISC	GOV	0	On January 23, 2014 a Human Resource Officer with the	2014	38.58178	-121.4921
206	3/27/2014	Sorenson Communicat	Salt Lake City	Utah	HACK	GOV	0	On March 7 it was discovered that there was an unauthc	2014	40.67918	-111.9176
208	04/02/2014	California Correctional	Tehachapi	California	PHYS	GOV	0	On March 9, 2014 an employee roster was discovered w	2014	35.13219	-118.449
219	05/06/2014	California Department	Rancho Cordov	California	PHYS	GOV	0	The California Department of Child Support Services ha	2014	38.58907	-121.3027
241	7/15/2014	City of Encinitas/San D	Encinitas	California	DISC	GOV	0	"City of Encinitas and San Dieguito Water District recent	2014	33.03699	-117.292
261	09/12/2014	Health and Human Ser	Napa	California	PORT	GOV	0	The Napa Health and Human Services Department, spec	2014	38.2986	-122.2862
279	11/25/2014	State Compensation In	Pleasanton	California	HACK	GOV	0	The State Compensation Insurance Fund, a state agency	2014	37.66243	-121.8747
307	04/02/2015	California Department	Sacramento	California	DISC	GOV	0	The California Department of Business Oversight notifie	2015	38.58157	-121.4944
310	04/06/2015	Tulare County Health a	Visalia	California	DISC	GOV	845	The Tulare County Health and Human Services Agency n	2015	36.27756	-119.3149
332	7/13/2015	Mule Creek State Priso	Ione	California	DISC	GOV	0	Mule Creek State Prison notified individuals of a breach	2015	38.36963	-120.9533
360	10/09/2015	Vacaville Housing Auth	Vacaville	California	DISC	GOV	0	The Vacaville Housing Authority (VHA) notified individu	2015	38.35705	-122.0017
371	11/09/2015	California Department	Sacramento	California	DISC	GOV	0	THe California Department of Motor Vehicles notified ii	2015	38.58157	-121.4944
394	1/26/2016	County of San Diego	San Diego	California	DISC	GOV	0	The County of San Diego Human Resources Department	2016	32.83385	-117.1309
461	07/06/2016	California Department	Stockton	California	DISC	GOV	0	"We are writing to you because of a security incident th	2016	37.89473	-121.1848
477	8/26/2016	County of Sacramento	Sacramento	California	DISC	GOV	0	"An error was discovered in the online automated appli	2016	38.58157	-121.4944

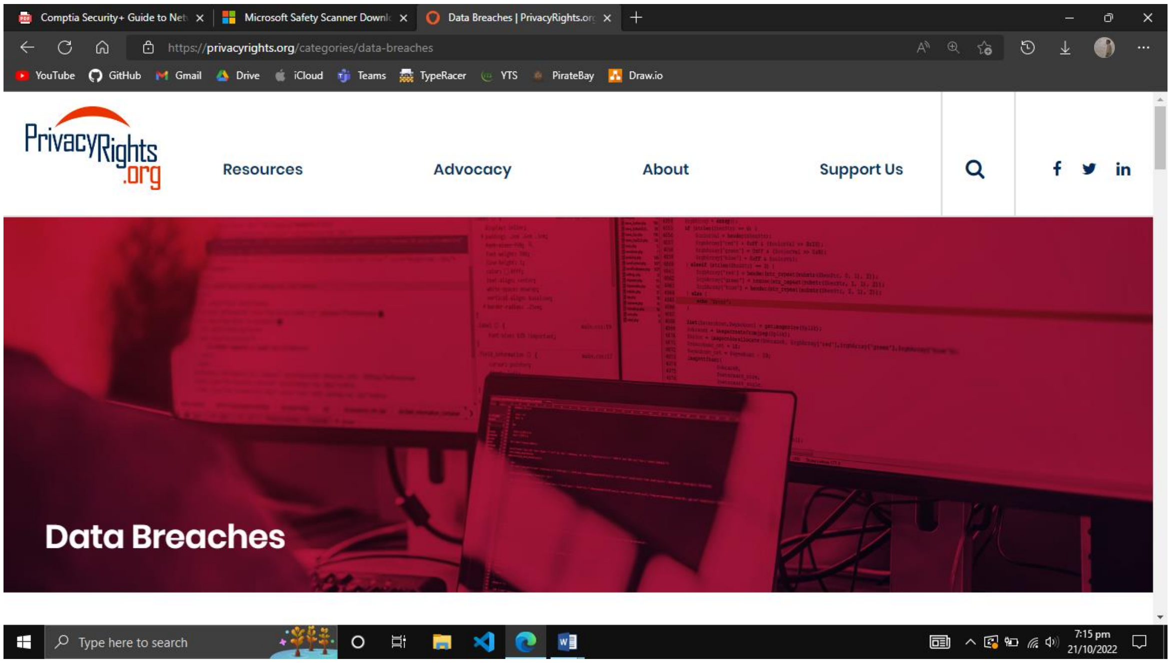
12. Under Select organization type(s), check GOV - Government & Military.



F1 — Type of organization

	A	B	C	D	E	F	G	H	K	L	M
1	Date Made Public	Company	City	State	Type of breach	Type of organization	Total Records	Description of incident	Year of Breach	Latitude	Longitude
13	3/31/2012	San Francisco Head Sta	San Francisco	California	UNKN	GOV	0	The San Francisco Head Start/Early Head Start database	2012	37.77493	-122.4194
27	05/11/2012	California Department	San Diego	California	HACK	GOV	0	In November 2011, hackers accessed and released priva	2012	32.71533	-117.1573
30	06/05/2012	California Department	Bakersfield	California	PHYS	GOV	0	The theft of a binder from an employee's car resulted ir	2012	35.37329	-119.0187
62	11/01/2012	Salinas Valley State Pri	Soledad	California	DISC	GOV	0	Sensitive staff information on a database file was founc	2012	36.42469	-121.3263
83	12/28/2012	East San Gabriel Valley	West Covina	California	DISC	GOV	0	A sensitive document was accidentally attached to an e	2012	34.06862	-117.939
139	07/03/2013	Bureau of Automotive	Rancho Cordov	California	HACK	GOV	0	An unauthorized individual accessed the network of a E	2013	38.58907	-121.3027
165	12/02/2013	Board of Barbering and	Sacramento	California	STAT	GOV	0	The August 23 office burglary of a desktop computer re:	2013	38.58157	-121.4944
189	2/20/2014	Department of Resour	Sacramento	California	DISC	GOV	0	On January 23, 2014 a Human Resource Officer with the	2014	38.58178	-121.4921
206	3/27/2014	Sorenson Communicat	Salt Lake City	Utah	HACK	GOV	0	On March 7 it was discovered that there was an unauthc	2014	40.67918	-111.9176
208	04/02/2014	California Correctional	Tehachapi	California	PHYS	GOV	0	On March 9, 2014 an employee roster was discovered w	2014	35.13219	-118.449
219	05/06/2014	California Department	Rancho Cordov	California	PHYS	GOV	0	The California Department of Child Support Services ha	2014	38.58907	-121.3027
241	7/15/2014	City of Encinitas/San D	Encinitas	California	DISC	GOV	0	"City of Encinitas and San Dieguito Water District recent	2014	33.03699	-117.292
261	09/12/2014	Health and Human Ser	Napa	California	PORT	GOV	0	The Napa Health and Human Services Department, spec	2014	38.2986	-122.2862
279	11/25/2014	State Compensation In	Pleasanton	California	HACK	GOV	0	The State Compensation Insurance Fund, a state agency	2014	37.66243	-121.8747
307	04/02/2015	California Department	Sacramento	California	DISC	GOV	0	The California Department of Business Oversight notifie	2015	38.58157	-121.4944
310	04/06/2015	Tulare County Health a	Visalia	California	DISC	GOV	845	The Tulare County Health and Human Services Agency n	2015	36.27756	-119.3149
332	7/13/2015	Mule Creek State Priso	Ione	California	DISC	GOV	0	Mule Creek State Prison notified individuals of a breach	2015	38.36963	-120.9533
360	10/09/2015	Vacaville Housing Auth	Vacaville	California	DISC	GOV	0	The Vacaville Housing Authority (VHA) notified individu	2015	38.35705	-122.0017
371	11/09/2015	California Department	Sacramento	California	DISC	GOV	0	THe California Department of Motor Vehicles notified ii	2015	38.58157	-121.4944
394	1/26/2016	County of San Diego	San Diego	California	DISC	GOV	0	The County of San Diego Human Resources Department	2016	32.83385	-117.1309
461	07/06/2016	California Department	Stockton	California	DISC	GOV	0	"We are writing to you because of a security incident th	2016	37.89473	-121.1848
477	8/26/2016	County of Sacramento	Sacramento	California	DISC	GOV	0	"An error was discovered in the online automated appli	2016	38.58157	-121.4944

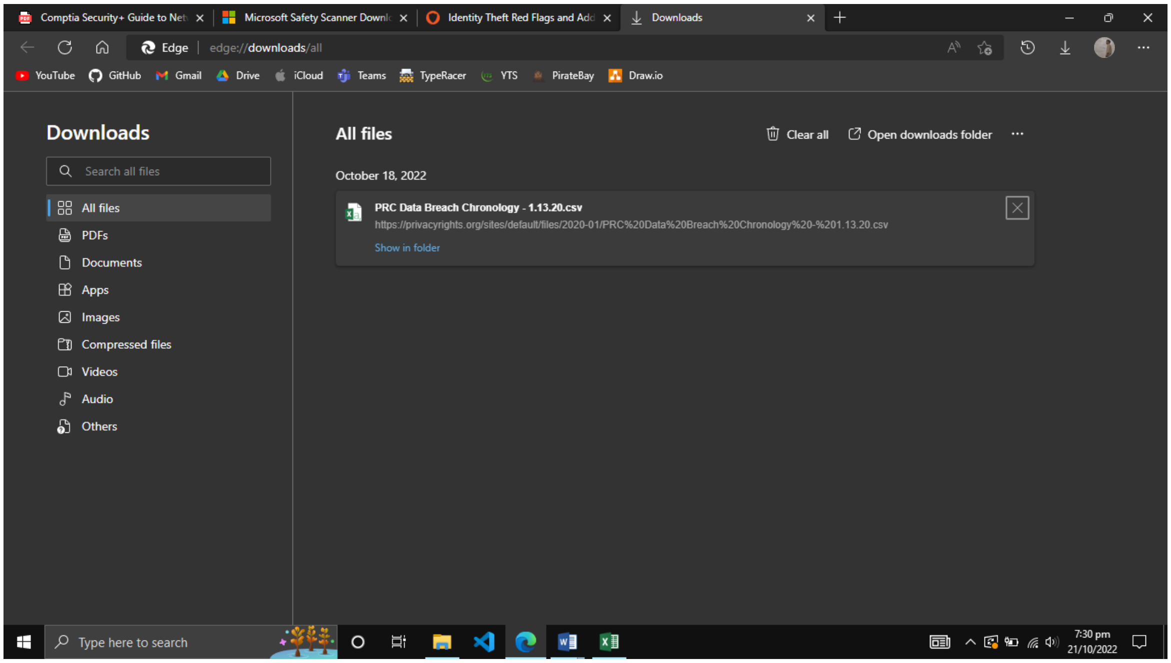
13. Click Search Data Breaches.



https://privacyrights.org/categories/data-breaches

Data Breaches

14. Read the Breach Subtotal by clicking the Download Results (CSV) file.



edge://downloads/all

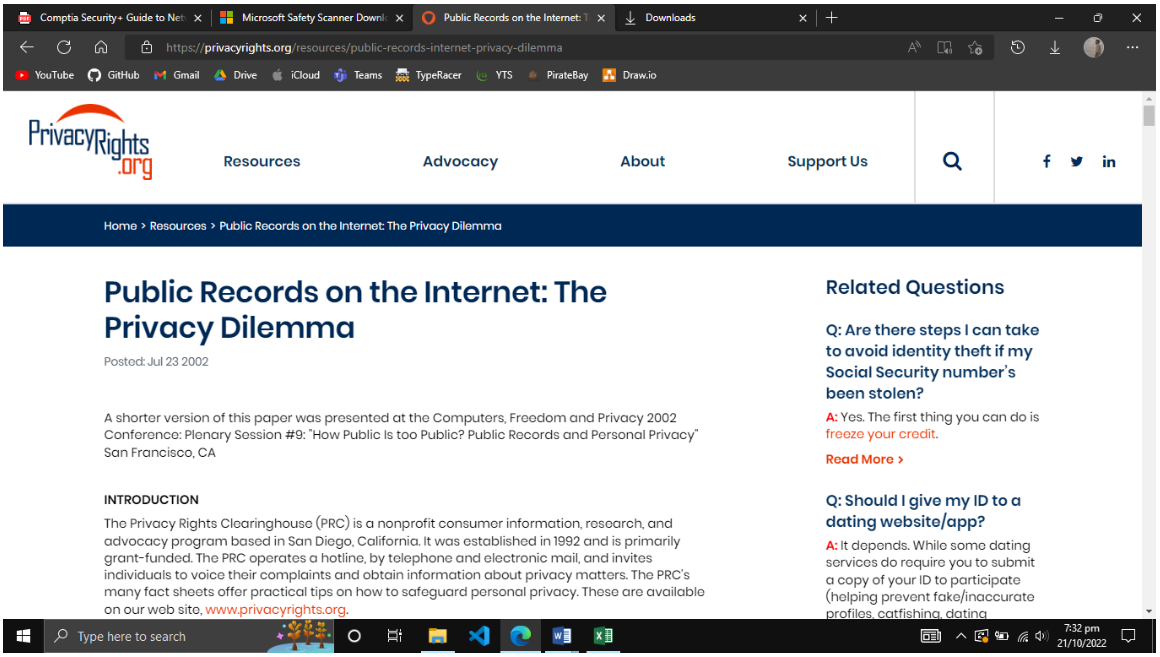
Downloads

All files

October 18, 2022

PRC Data Breach Chronology - 1.13.20.csv
https://privacyrights.org/sites/default/files/2020-01/PRC%20Data%20Breach%20Chronology%20-%201.13.20.csv
Show in folder

15. Open the file and then scroll down the different breaches. What should the government be doing to limit these breaches?


Comptia Security+ Guide to Net
Microsoft Safety Scanner Downl
Public Records on the Internet: T
Downloads
https://privacyrights.org/resources/public-records-internet-privacy-dilemma
YouTube
GitHub
Gmail
Drive
iCloud
Teams
TypeRacer
YTS
PirateBay
Draw.io
PrivacyRights.org
Resources
Advocacy
About
Support Us
Home > Resources > Public Records on the Internet: The Privacy Dilemma
Type here to search
7:32 pm
21/10/2022

Public Records on the Internet: The Privacy Dilemma

Posted: Jul 23 2002

A shorter version of this paper was presented at the Computers, Freedom and Privacy 2002 Conference: Plenary Session #9: "How Public Is too Public? Public Records and Personal Privacy" San Francisco, CA

INTRODUCTION

The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer information, research, and advocacy program based in San Diego, California. It was established in 1992 and is primarily grant-funded. The PRC operates a hotline, by telephone and electronic mail, and invites individuals to voice their complaints and obtain information about privacy matters. The PRC's many fact sheets offer practical tips on how to safeguard personal privacy. These are available on our web site, www.privacyrights.org.

Related Questions

Q: Are there steps I can take to avoid identity theft if my Social Security number's been stolen?

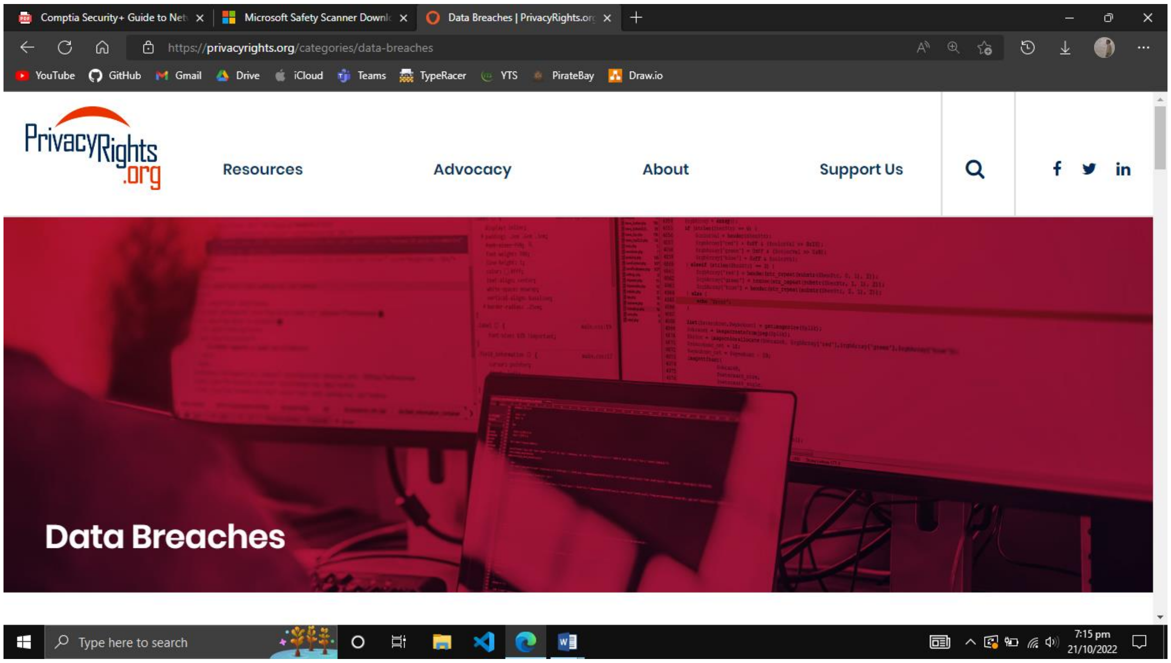
A: Yes. The first thing you can do is freeze your credit.

Read More >

Q: Should I give my ID to a dating website/app?

A: It depends. While some dating services do require you to submit a copy of your ID to participate (helping prevent fake/inaccurate profiles, catfishing, dating

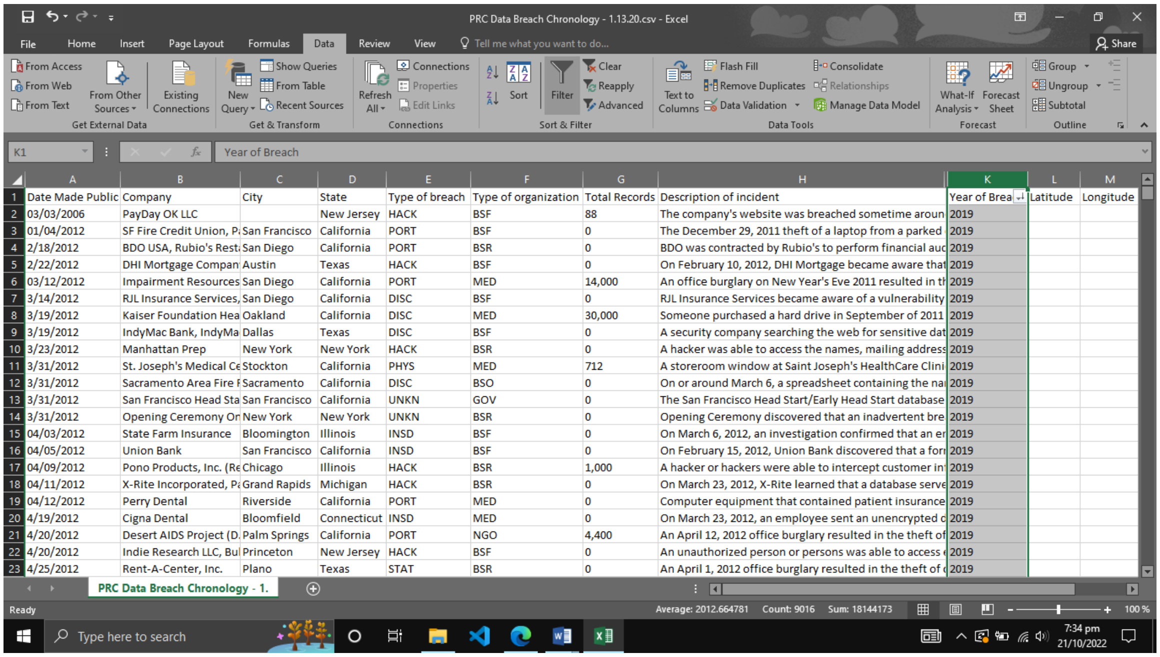
16. Scroll back to the top of the page. Click New Data Breach Search.



Data Breaches

17. Now create a search based on criteria that you are interested in, such as the Payment Card Fraud against Retail/Merchants during the current year.

    Data for 2022 was not provided in database file.



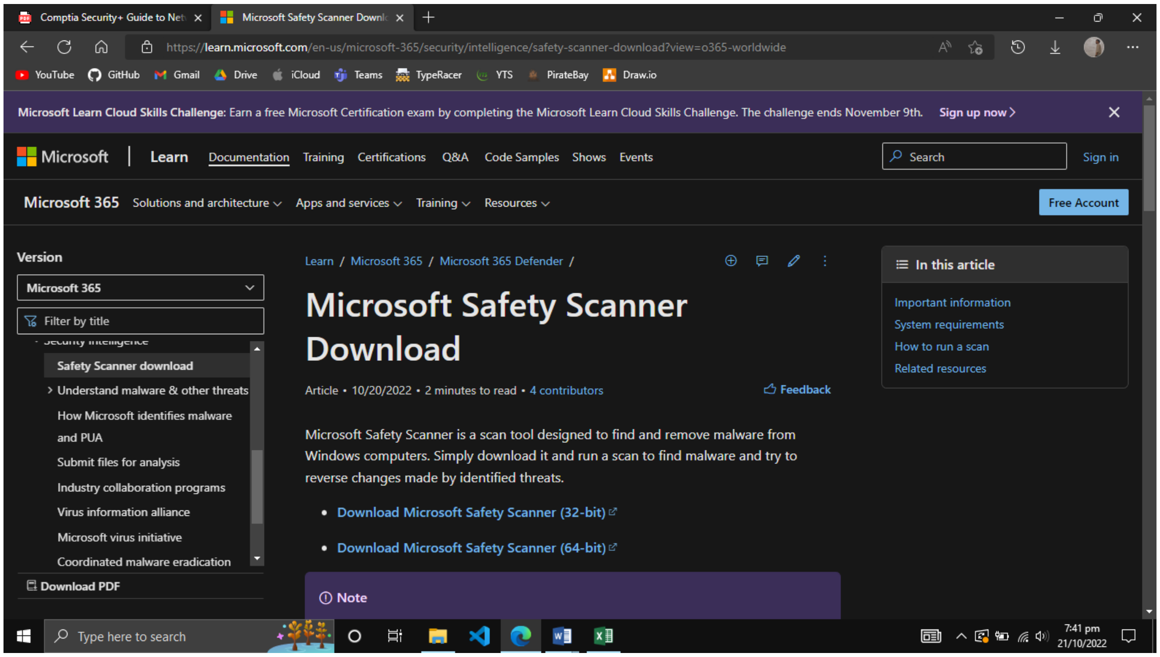
	A	B	C	D	E	F	G	H	K	L	M
1	Date Made Public	Company	City	State	Type of breach	Type of organization	Total Records	Description of incident	Year of Brea	Latitude	Longitude
2	03/03/2006	PayDay OK LLC		New Jersey	HACK	BSF	88	The company's website was breached sometime aroun	2019		
3	01/04/2012	SF Fire Credit Union, Pa	San Francisco	California	PORT	BSF	0	The December 29, 2011 theft of a laptop from a parked	2019		
4	2/18/2012	BDO USA, Rubio's Resta	San Diego	California	PORT	BSR	0	BDO was contracted by Rubio's to perform financial auc	2019		
5	2/22/2012	DHI Mortgage Compan	Austin	Texas	HACK	BSF	0	On February 10, 2012, DHI Mortgage became aware that	2019		
6	03/12/2012	Impairment Resources	San Diego	California	PORT	MED	14,000	An office burglary on New Year's Eve 2011 resulted in th	2019		
7	3/14/2012	RJL Insurance Services,	San Diego	California	DISC	BSF	0	RJL Insurance Services became aware of a vulnerability	2019		
8	3/19/2012	Kaiser Foundation Hea	Oakland	California	DISC	MED	30,000	Someone purchased a hard drive in September of 2011	2019		
9	3/19/2012	IndyMac Bank, IndyMa	Dallas	Texas	DISC	BSF	0	A security company searching the web for sensitive dat	2019		
10	3/23/2012	Manhattan Prep	New York	New York	HACK	BSR	0	A hacker was able to access the names, mailing address	2019		
11	3/31/2012	St. Joseph's Medical Ce	Stockton	California	PHYS	MED	712	A storeroom window at Saint Joseph's HealthCare Clini	2019		
12	3/31/2012	Sacramento Area Fire F	Sacramento	California	DISC	BSO	0	On or around March 6, a spreadsheet containing the nai	2019		
13	3/31/2012	San Francisco Head Sta	San Francisco	California	UNKN	GOV	0	The San Francisco Head Start/Early Head Start database	2019		
14	3/31/2012	Opening Ceremony On	New York	New York	UNKN	BSR	0	Opening Ceremony discovered that an inadvertent bre	2019		
15	04/03/2012	State Farm Insurance	Bloomington	Illinois	INSD	BSF	0	On March 6, 2012, an investigation confirmed that an er	2019		
16	04/05/2012	Union Bank	San Francisco	California	INSD	BSF	0	On February 15, 2012, Union Bank discovered that a forı	2019		
17	04/09/2012	Pono Products, Inc. (Re	Chicago	Illinois	HACK	BSR	1,000	A hacker or hackers were able to intercept customer int	2019		
18	04/11/2012	X-Rite Incorporated, Pa	Grand Rapids	Michigan	HACK	BSR	0	On March 23, 2012, X-Rite learned that a database serve	2019		
19	04/12/2012	Perry Dental	Riverside	California	PORT	MED	0	Computer equipment that contained patient insurance	2019		
20	4/19/2012	Cigna Dental	Bloomfield	Connecticut	INSD	MED	0	On March 23, 2012, an employee sent an unencrypted c	2019		
21	4/20/2012	Desert AIDS Project (D.	Palm Springs	California	PORT	NGO	4,400	An April 12, 2012 office burglary resulted in the theft of	2019		
22	4/20/2012	Indie Research LLC, Bul	Princeton	New Jersey	HACK	BSF	0	An unauthorized person or persons was able to access e	2019		
23	4/25/2012	Rent-A-Center, Inc.	Plano	Texas	STAT	BSR	0	An April 1, 2012 office burglary resulted in the theft of (	2019		

18. When finished, close all windows.

Project 1-3: *Scanning for Malware using Microsoft Safety Scanner*

In this project, you download and run the Microsoft Safety Scanner to determine if there is any malware on the computer.

1. Determine which system type of Windows you are running. Click Start, Settings, System, and then About this PC. Look under System type for the description. Open your web browser and enter the URL www.microsoft.com/security/scanner /en-us/default.asp (if you are no longer able to access the site through the URL, use a search engine to search for "Microsoft Safety Scanner").


Comptia Security+ Guide to Net
Microsoft Safety Scanner Downl
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide
YouTube
GitHub
Gmail
Drive
iCloud
Teams
TypeRacer
YTS
PirateBay
Draw.io
Microsoft
Learn
Documentation
Training
Certifications
Q&A
Code Samples
Shows
Events
Search
Sign in
Microsoft 365
Solutions and architecture
Apps and services
Training
Resources
Free Account
Version
Microsoft 365
Filter by title
Security intelligence
Safety Scanner download
Understand malware & other threats
How Microsoft identifies malware and PUA
Submit files for analysis
Industry collaboration programs
Virus information alliance
Microsoft virus initiative
Coordinated malware eradication
Download PDF
Learn / Microsoft 365 / Microsoft 365 Defender /
In this article
Important information
System requirements
How to run a scan
Related resources
Feedback
Type here to search
7:41 pm
21/10/2022

Microsoft Learn Cloud Skills Challenge: Earn a free Microsoft Certification exam by completing the Microsoft Learn Cloud Skills Challenge. The challenge ends November 9th. Sign up now >

Microsoft Safety Scanner Download

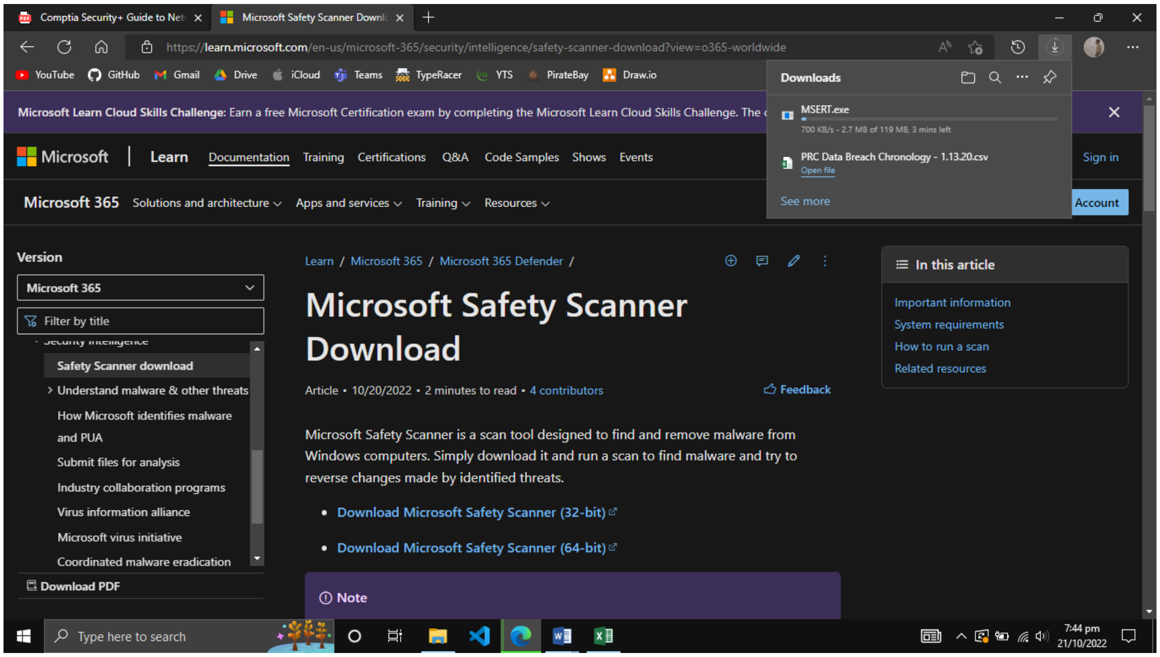
Article • 10/20/2022 • 2 minutes to read • 4 contributors

Microsoft Safety Scanner is a scan tool designed to find and remove malware from Windows computers. Simply download it and run a scan to find malware and try to reverse changes made by identified threats.

- Download Microsoft Safety Scanner (32-bit)
- Download Microsoft Safety Scanner (64-bit)

ⓘ Note

2. Click Download Now.
3. Select either 32-bit or 64-bit, depending upon which system type of Windows you are running.


Comptia Security+ Guide to Net
Microsoft Safety Scanner Downl
https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide
YouTube
GitHub
Gmail
Drive
iCloud
Teams
TypeRacer
YTS
PirateBay
Draw.io
Downloads
See more
Microsoft
Learn
Documentation
Training
Certifications
Q&A
Code Samples
Shows
Events
Sign in
Microsoft 365
Solutions and architecture
Apps and services
Training
Resources
Account
Version
Microsoft 365
Filter by title
Security intelligence
Safety Scanner download
Understand malware & other threats
How Microsoft identifies malware and PUA
Submit files for analysis
Industry collaboration programs
Virus information alliance
Microsoft virus initiative
Coordinated malware eradication
Download PDF
Learn / Microsoft 365 / Microsoft 365 Defender /
Feedback
In this article
Important information
System requirements
How to run a scan
Related resources
Note
Type here to search
7:44 pm
21/10/2022

Microsoft Learn Cloud Skills Challenge: Earn a free Microsoft Certification exam by completing the Microsoft Learn Cloud Skills Challenge. The

MSERT.exe
700 KB/s - 2.7 MB of 119 MB, 3 mins left

PRC Data Breach Chronology - 1.13.20.csv
Open file

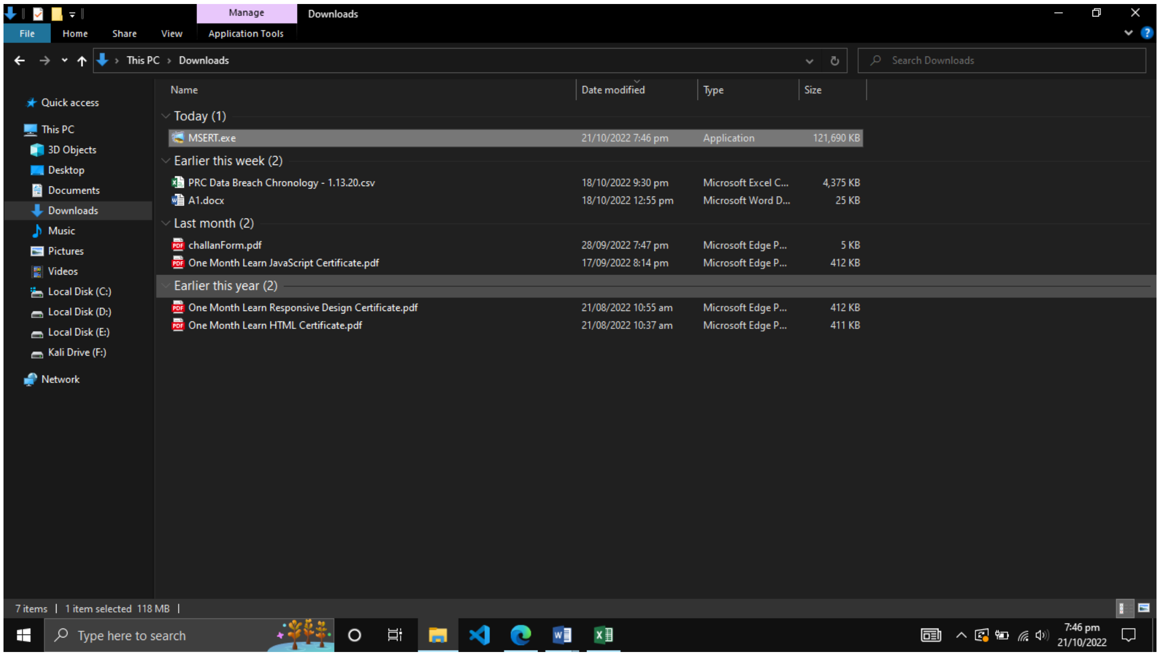
Microsoft Safety Scanner Download

Article • 10/20/2022 • 2 minutes to read • 4 contributors

Microsoft Safety Scanner is a scan tool designed to find and remove malware from Windows computers. Simply download it and run a scan to find malware and try to reverse changes made by identified threats.

- Download Microsoft Safety Scanner (32-bit)
- Download Microsoft Safety Scanner (64-bit)

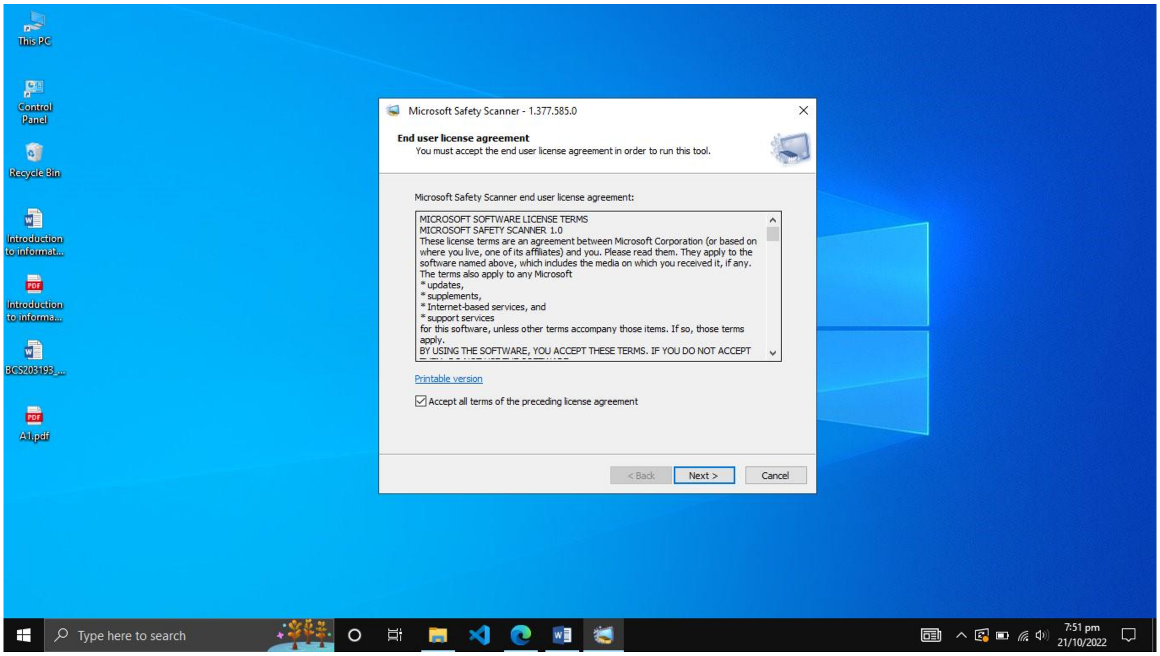
4. When the program finishes downloading, right-click Start and click File Explorer.



Name	Date modified	Type	Size
Today (1)			
MSERT.exe	21/10/2022 7:46 pm	Application	121,690 KB
Earlier this week (2)			
PRC Data Breach Chronology - 1.13.20.csv	18/10/2022 9:30 pm	Microsoft Excel C...	4,375 KB
A1.docx	18/10/2022 12:55 pm	Microsoft Word D...	25 KB
Last month (2)			
challanForm.pdf	28/09/2022 7:47 pm	Microsoft Edge P...	5 KB
One Month Learn JavaScript Certificate.pdf	17/09/2022 8:14 pm	Microsoft Edge P...	412 KB
Earlier this year (2)			
One Month Learn Responsive Design Certificate.pdf	21/08/2022 10:55 am	Microsoft Edge P...	412 KB
One Month Learn HTML Certificate.pdf	21/08/2022 10:37 am	Microsoft Edge P...	411 KB

7 items | 1 item selected 118 MB |

5. Click the Downloads icon in the left pane.
6. Double-click the msert.exe file.
7. If the User Account Control dialog box appears, click Yes. Click Run.
8. Click the check box to accept the license terms for this software. Click Next.



Microsoft Safety Scanner - 1.377.585.0

End user license agreement

You must accept the end user license agreement in order to run this tool.

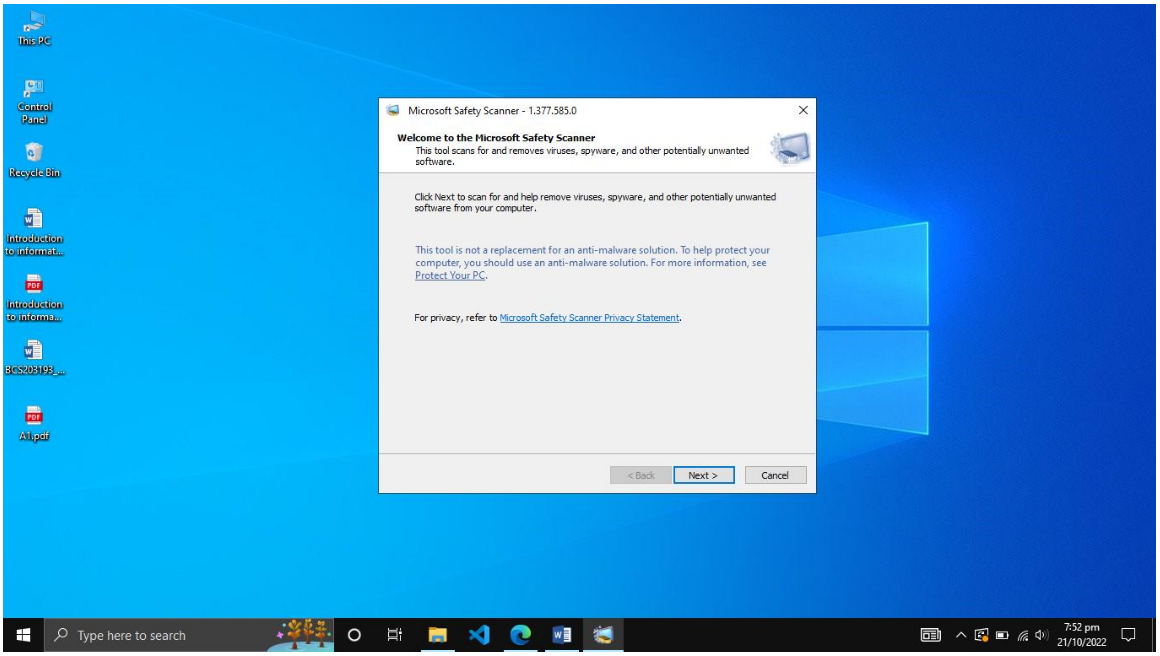
Microsoft Safety Scanner end user license agreement:

MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT SAFETY SCANNER 1.0
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
* updates,
* supplements,
* Internet-based services, and
* support services
for this software, unless other terms accompany those items. If so, those terms apply.
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT

Printable version

☑ Accept all terms of the preceding license agreement

9. Click Next.



Microsoft Safety Scanner - 1.377.585.0

Welcome to the Microsoft Safety Scanner

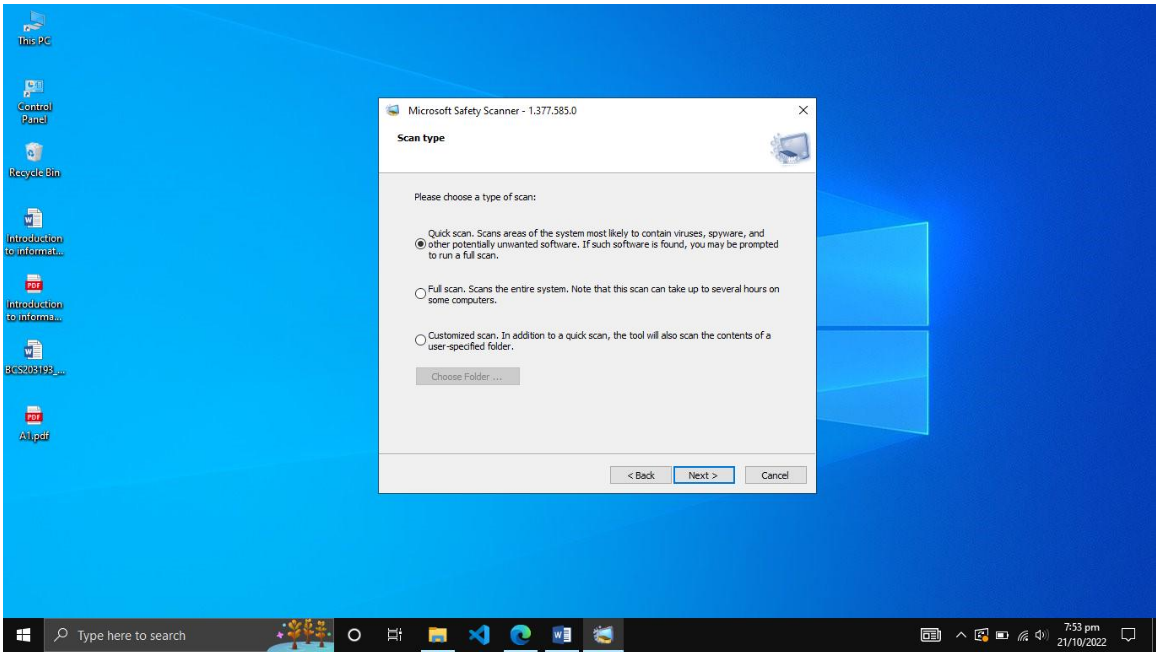
This tool scans for and removes viruses, spyware, and other potentially unwanted software.

Click Next to scan for and help remove viruses, spyware, and other potentially unwanted software from your computer.

This tool is not a replacement for an anti-malware solution. To help protect your computer, you should use an anti-malware solution. For more information, see Protect Your PC.

For privacy, refer to Microsoft Safety Scanner Privacy Statement.

10. Select Quick scan if necessary.



Microsoft Safety Scanner - 1.377.585.0

Scan type

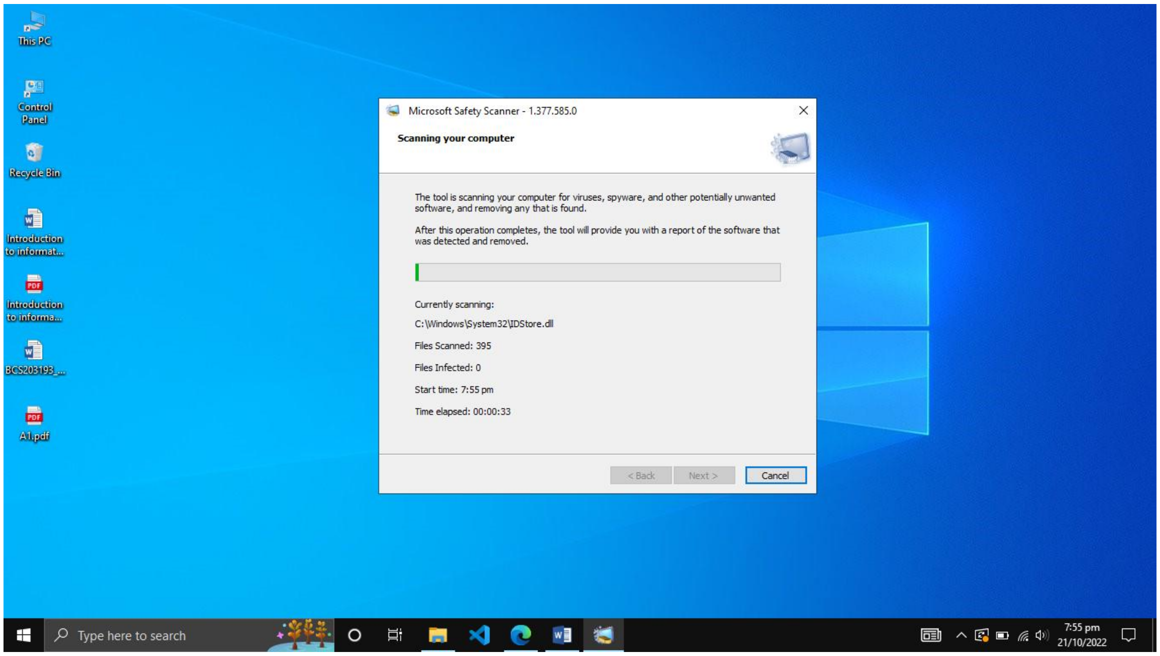
Please choose a type of scan:

● Quick scan. Scans areas of the system most likely to contain viruses, spyware, and other potentially unwanted software. If such software is found, you may be prompted to run a full scan.

○ Full scan. Scans the entire system. Note that this scan can take up to several hours on some computers.

○ Customized scan. In addition to a quick scan, the tool will also scan the contents of a user-specified folder.

11. Click Next.



Microsoft Safety Scanner - 1.377.585.0

Scanning your computer

The tool is scanning your computer for viruses, spyware, and other potentially unwanted software, and removing any that is found.

After this operation completes, the tool will provide you with a report of the software that was detected and removed.

Currently scanning:

C:\Windows\System32\IDStore.dll

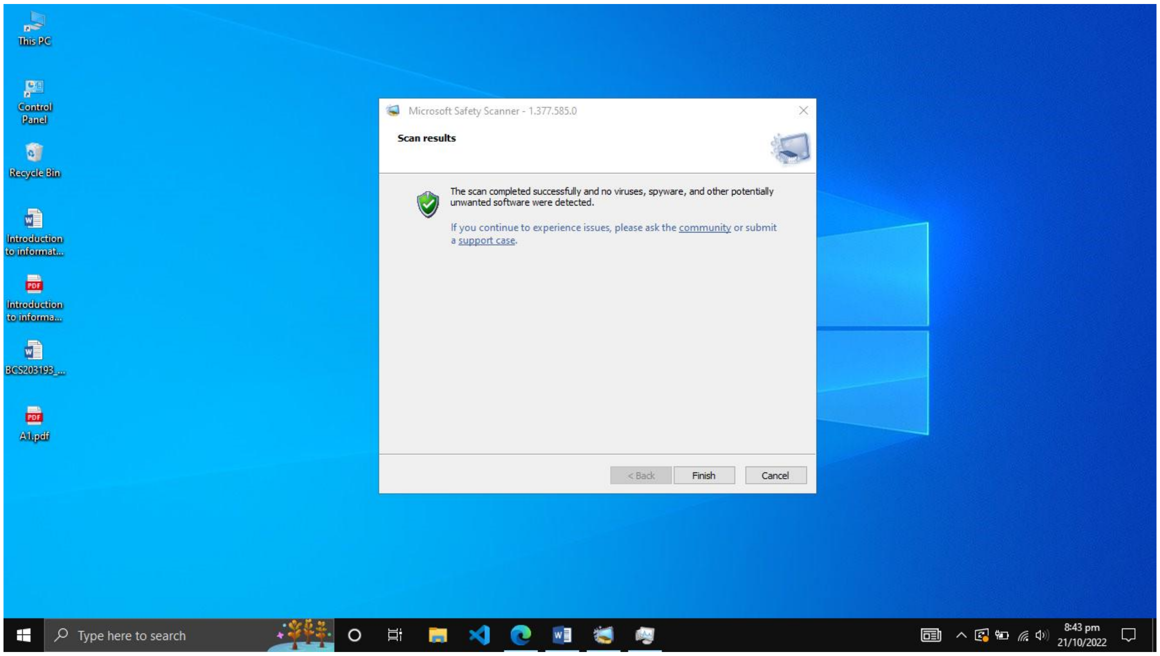
Files Scanned: 395

Files Infected: 0

Start time: 7:55 pm

Time elapsed: 00:00:33

12. Depending on your computer this scan may take several minutes. Analyze the results of the scan to determine if there is any malicious software found in your computer.



The scan completed successfully and no viruses, spyware, and other potentially unwanted software were detected.

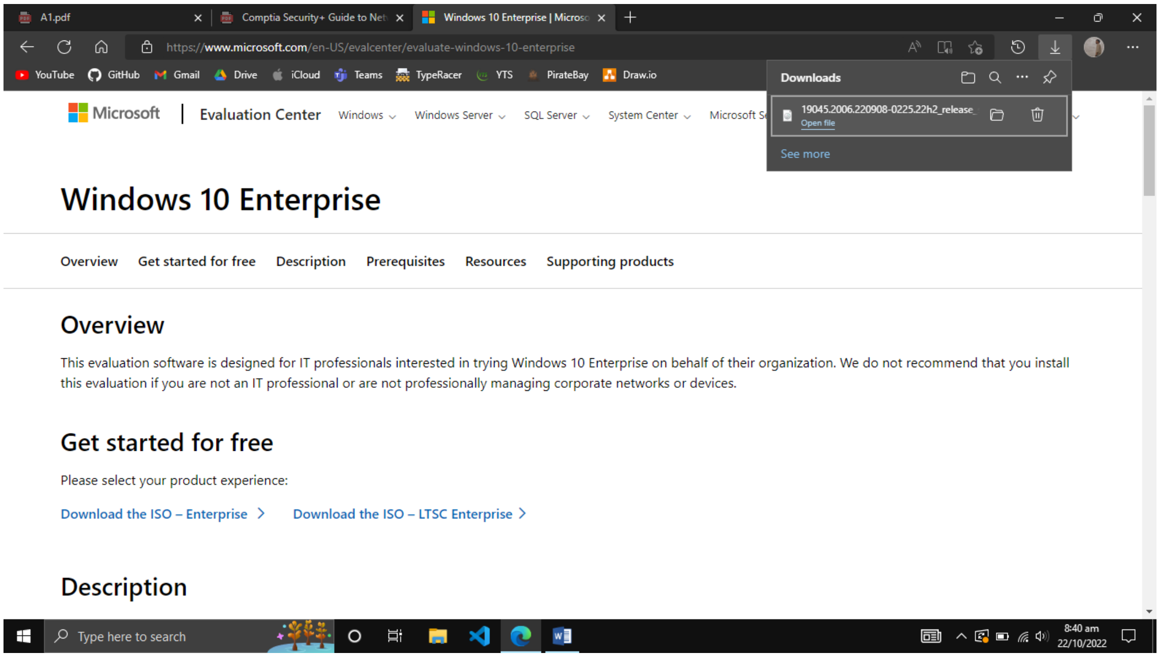
If you continue to experience issues, please ask the community or submit a support case.

13. If you have problems, you can click View detailed results of the scan. After reviewing the results, click OK. If you do not find any problems, click Finish.
14. If any malicious software was found on your computer run the scan again and select Full scan. After the scan is complete, click Finish to close the dialog box.
15. Close all windows.

Project 1-5: *Creating a Virtual Machine of Windows 10 for Security Testing (using VMware)*

After installing VMware the next step is to create the guest operating system. For this project Windows 10 will be installed.

1. Obtain the ISO image of Windows 10 using one of the options above and save it on the hard drive of the computer.



Windows 10 Enterprise

Overview

This evaluation software is designed for IT professionals interested in trying Windows 10 Enterprise on behalf of their organization. We do not recommend that you install this evaluation if you are not an IT professional or are not professionally managing corporate networks or devices.

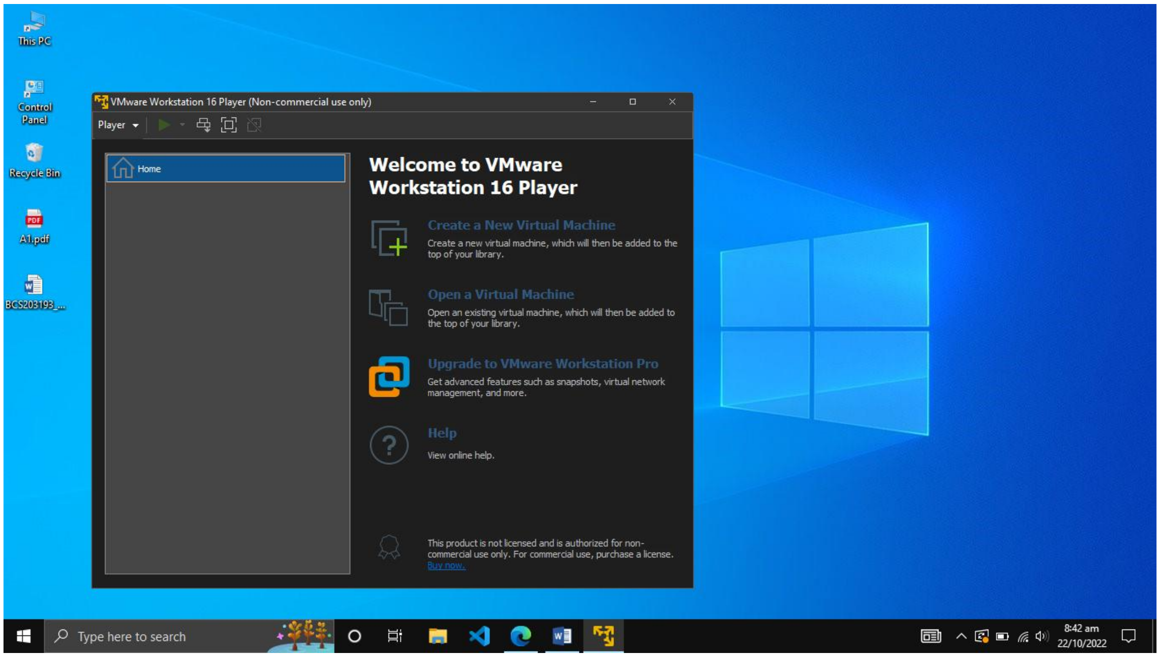
Get started for free

Please select your product experience:

Download the ISO – Enterprise >   Download the ISO – LTSC Enterprise >

Description

2. Launch VMware.



Welcome to VMware Workstation 16 Player

Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.

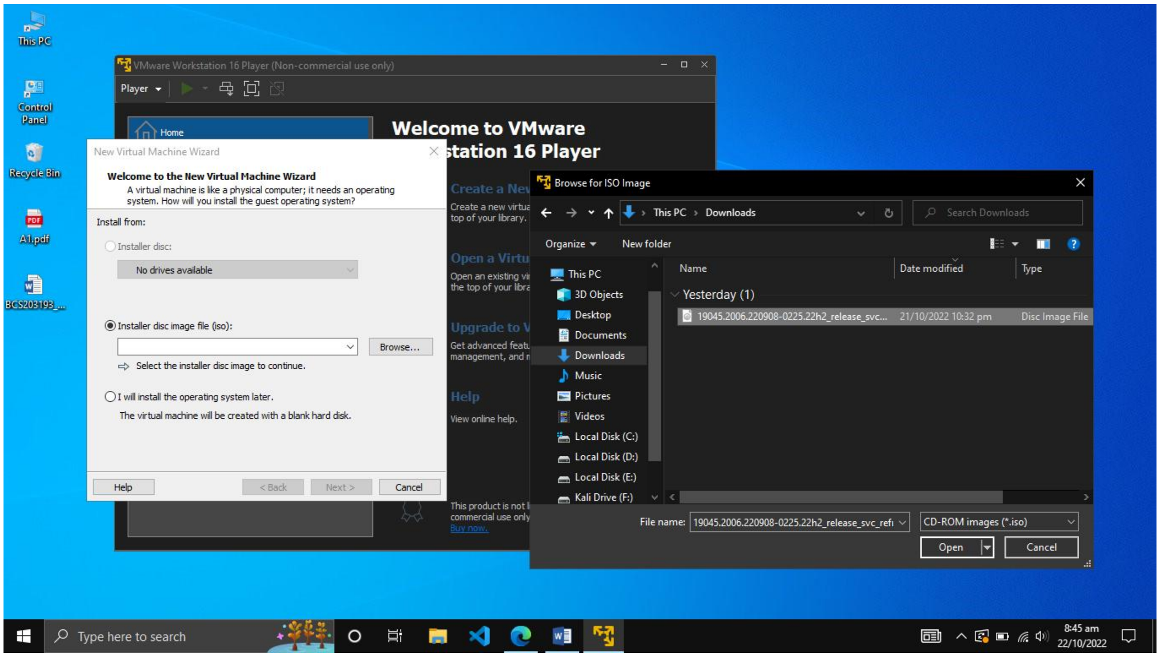
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.

Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.

Help
View online help.

This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license. Buy now.

3. Click Create a New Virtual Machine and Select ISO file of Windows 10.



New Virtual Machine Wizard

Welcome to the New Virtual Machine Wizard

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

Select the installer disc image to continue.

○ I will install the operating system later.

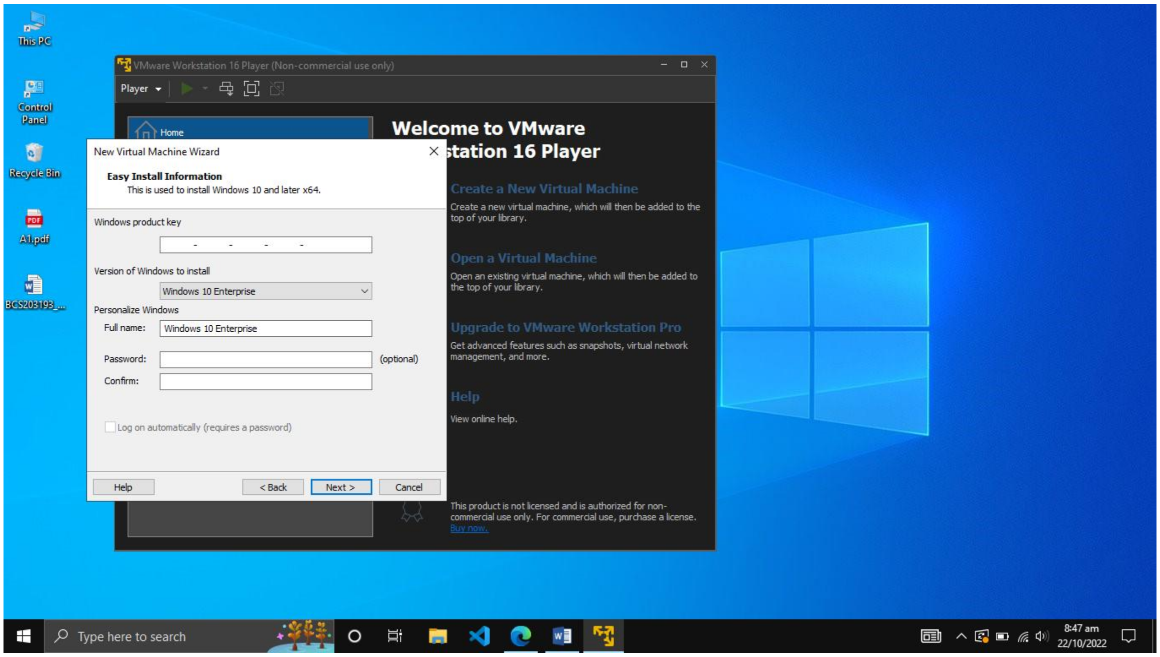
The virtual machine will be created with a blank hard disk.

Browse for ISO Image

File name: 19045.2006.220908-0225.22h2_release_svc_refr

Name	Date modified	Type
19045.2006.220908-0225.22h2_release_svc...	21/10/2022 10:32 pm	Disc Image File

4. In Full Name: enter Windows 10 as the name of the virtual machine.



New Virtual Machine Wizard

Easy Install Information

This is used to install Windows 10 and later x64.

Windows product key

Version of Windows to install: Windows 10 Enterprise

Personalize Windows

Full name: Windows 10 Enterprise

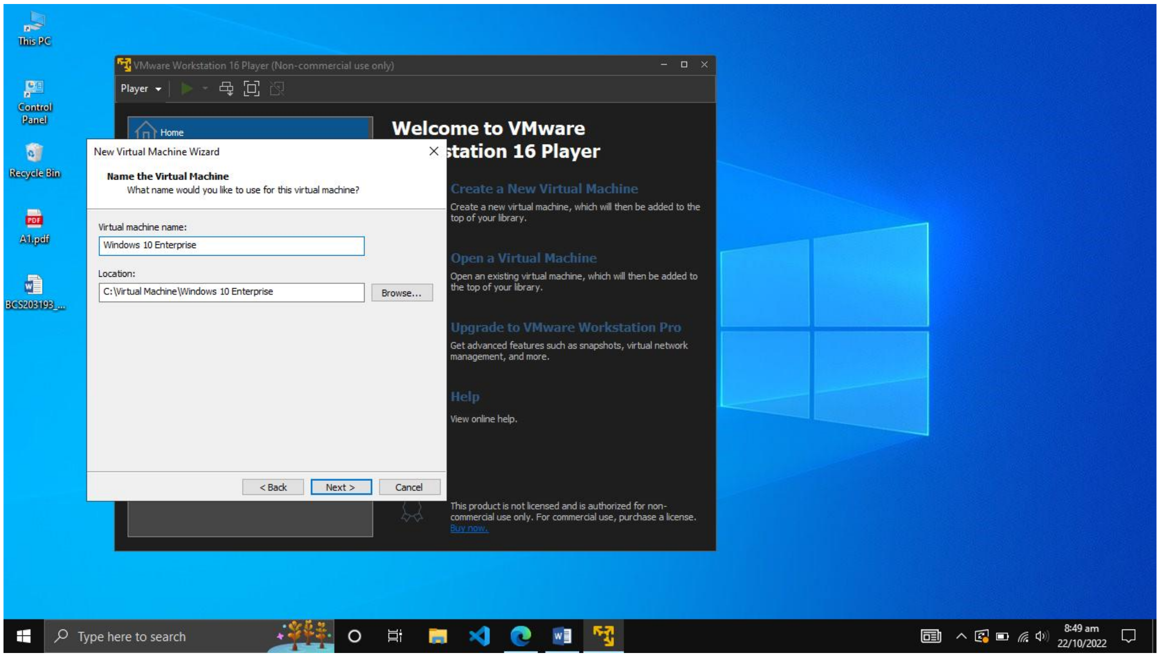
Password: (optional)

Confirm:

□ Log on automatically (requires a password)

This PC
Control Panel
Recycle Bin
A1.pdf
BCS203193_...
VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Welcome to VMware
station 16 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license.
Buy now.
Help
< Back
Next >
Cancel
Type here to search
8:47 am
22/10/2022

5. Enter the name of Virtual Machine, select location and Click Next.



New Virtual Machine Wizard

Name the Virtual Machine

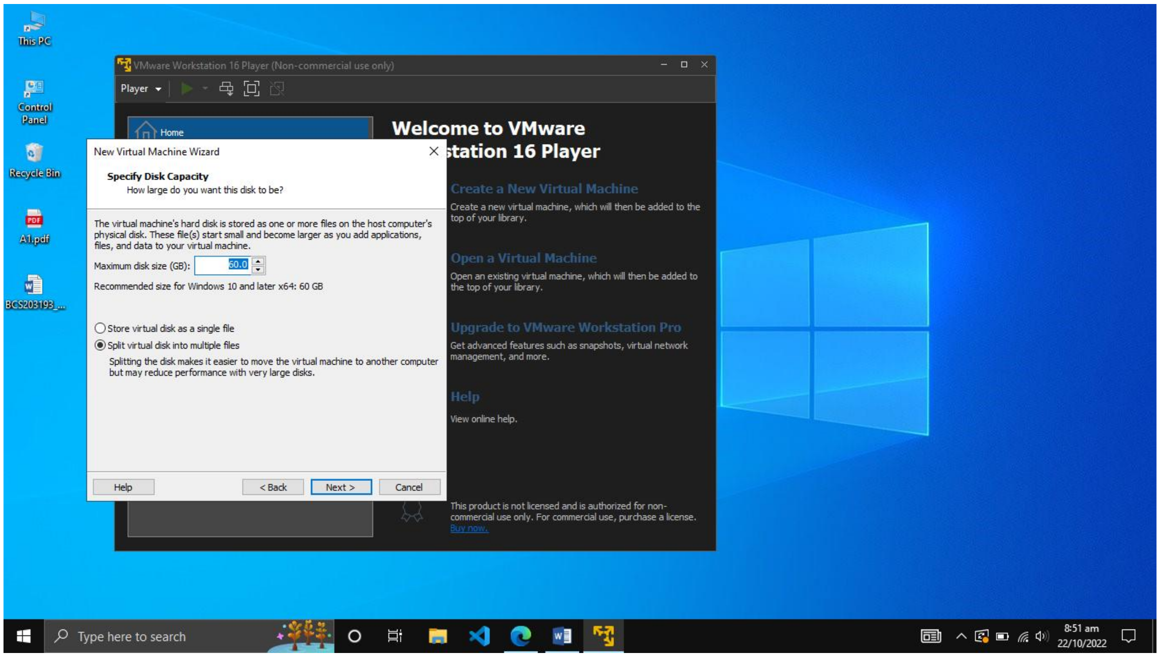
What name would you like to use for this virtual machine?

Virtual machine name: Windows 10 Enterprise

Location: C:\Virtual Machine\Windows 10 Enterprise

This PC
Control Panel
Recycle Bin
A1.pdf
BCS203193_...
VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Welcome to VMware Workstation 16 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license.
Buy now.
Browse...
< Back
Next >
Cancel
Type here to search
8:49 am
22/10/2022

6. Specify Disk Capacity and Click next.



New Virtual Machine Wizard

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 60.0

Recommended size for Windows 10 and later x64: 60 GB

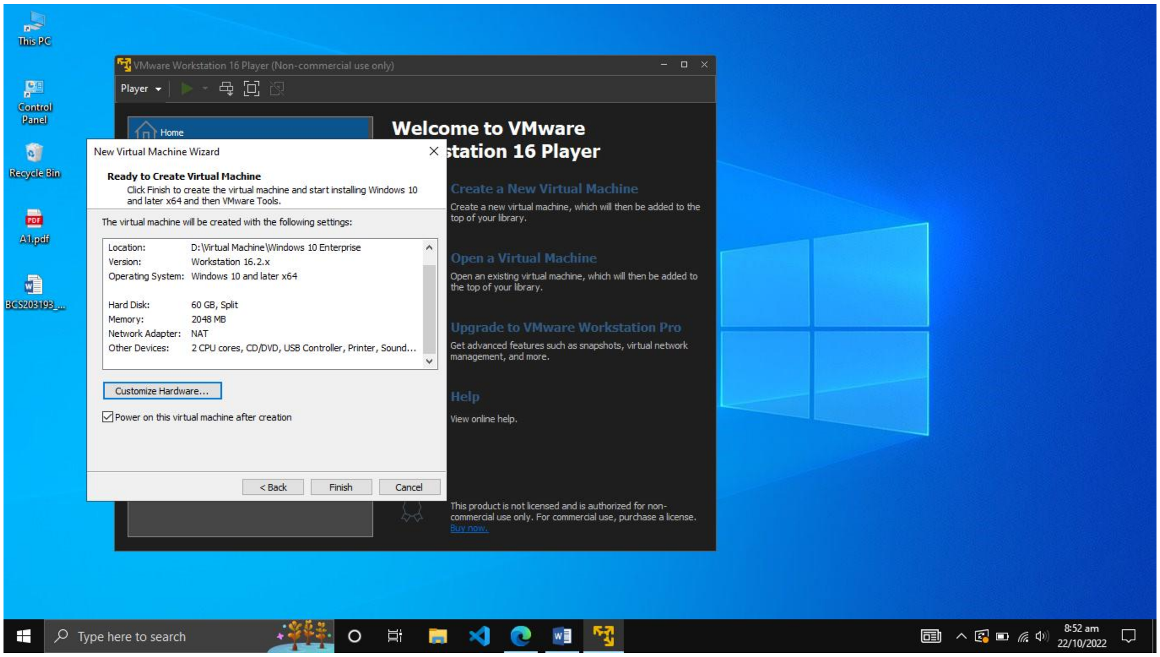
○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

This PC
Control Panel
Recycle Bin
A1.pdf
BCS203193_...
VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Welcome to VMware Workstation 16 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license.
Buy now.
Help
< Back
Next >
Cancel
Type here to search
8:51 am
22/10/2022

7. Under Memory size accept the recommended size or increase the allocation if you have sufficient RAM on your computer. Click Next.



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Windows 10 and later x64 and then VMware Tools.

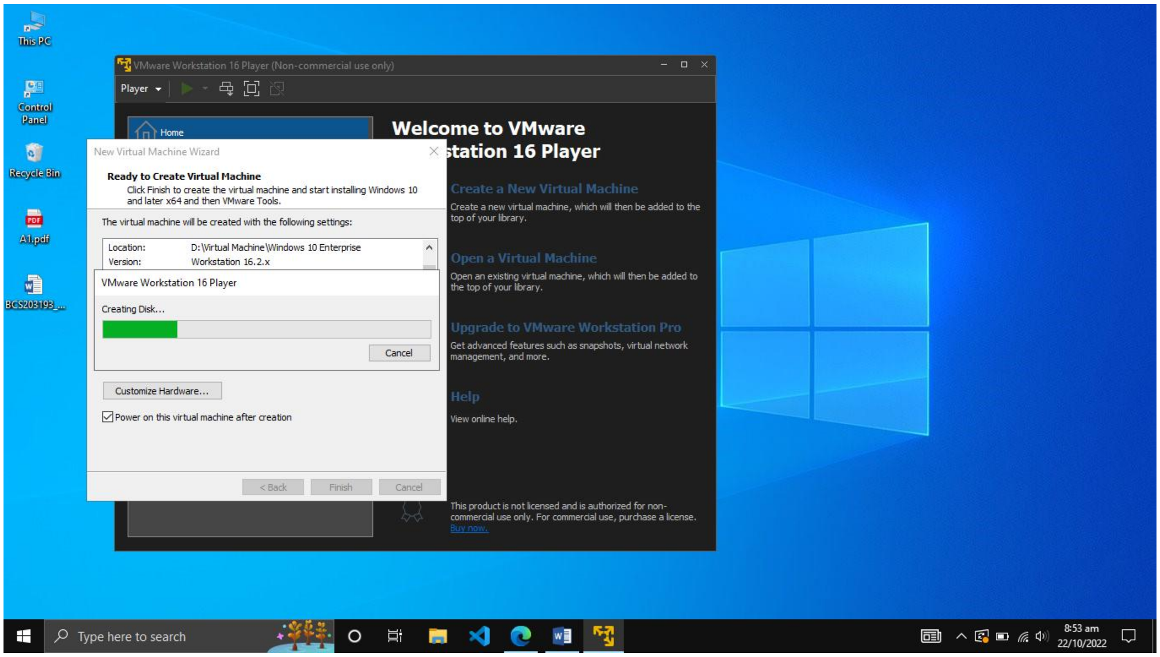
The virtual machine will be created with the following settings:

```
Location:          D:\Virtual Machine\Windows 10 Enterprise
Version:           Workstation 16.2.x
Operating System:  Windows 10 and later x64

Hard Disk:         60 GB, Split
Memory:            2048 MB
Network Adapter:   NAT
Other Devices:     2 CPU cores, CD/DVD, USB Controller, Printer, Sound...
```

☑ Power on this virtual machine after creation

This PC
Control Panel
Recycle Bin
A1.pdf
BCS203193_...
VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Welcome to VMware Workstation 16 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license.
Buy now.
Customize Hardware...
< Back
Finish
Cancel
Type here to search
8:52 am
22/10/2022

8. Under Hard disk accept Create a virtual hard drive now. Click Create.



New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine and start installing Windows 10 and later x64 and then VMware Tools.

The virtual machine will be created with the following settings:

```
Location:          D:\Virtual Machine\Windows 10 Enterprise
Version:           Workstation 16.2.x
```

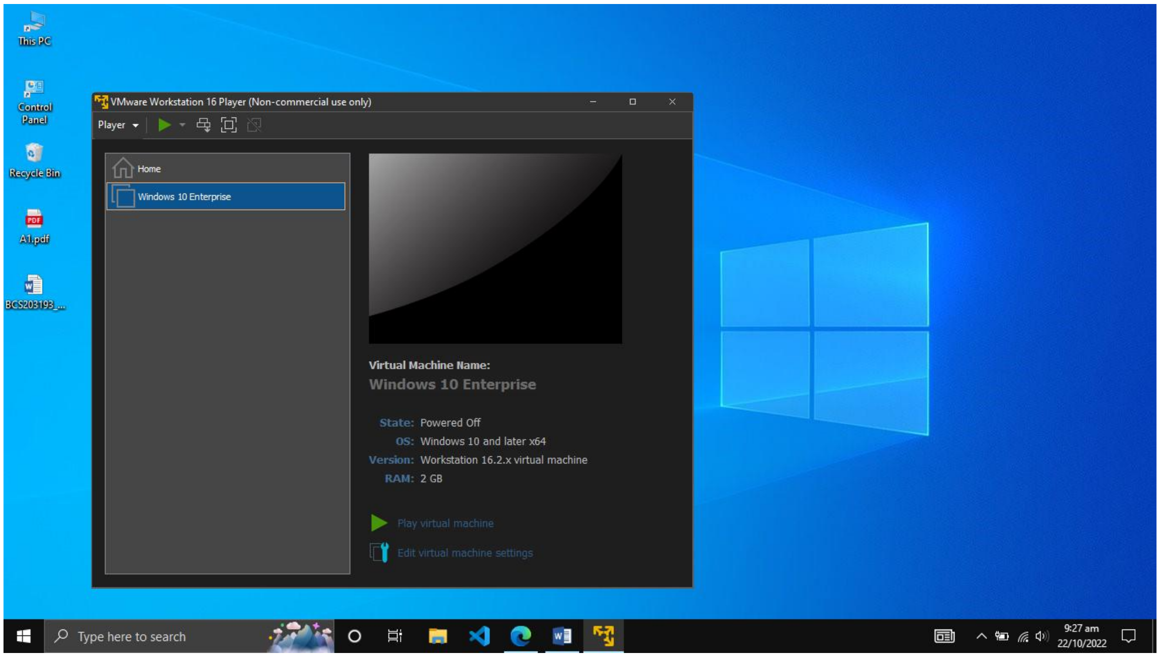
VMware Workstation 16 Player

Creating Disk...

☑ Power on this virtual machine after creation

This PC
Control Panel
Recycle Bin
A1.pdf
BCS203193_...
VMware Workstation 16 Player (Non-commercial use only)
Player
Home
Welcome to VMware Workstation 16 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is authorized for non-commercial use only. For commercial use, purchase a license.
Buy now.
Cancel
Customize Hardware...
< Back
Finish
Cancel
Type here to search
8:53 am
22/10/2022

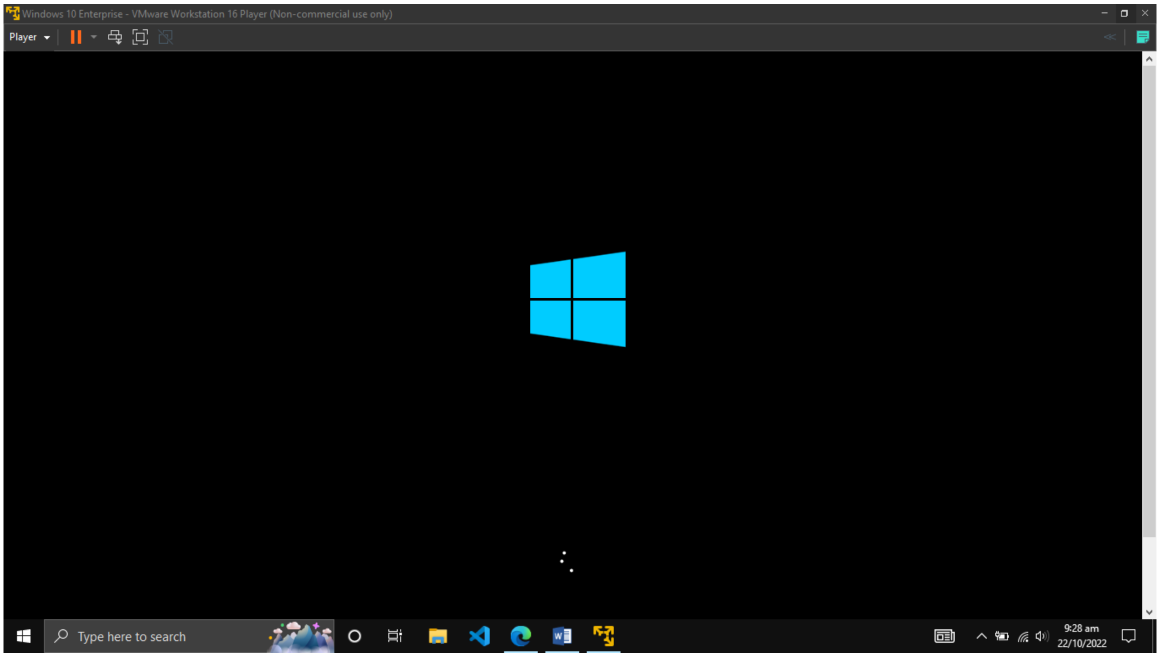
9. Play the Virtual Machine



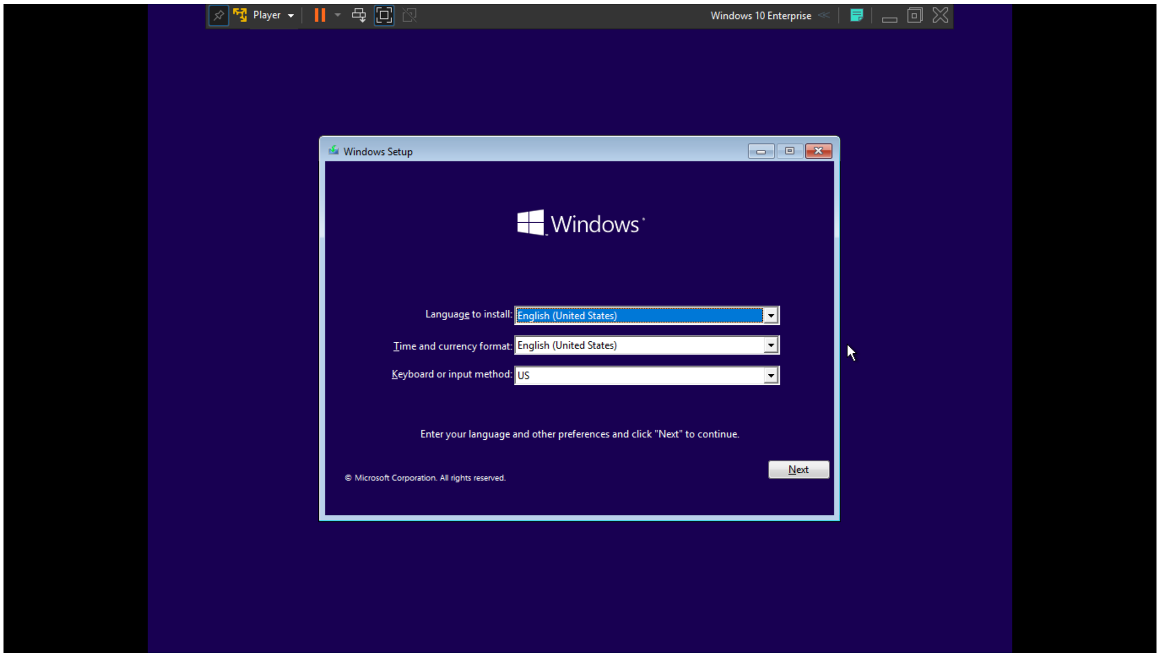
Virtual Machine Name:
Windows 10 Enterprise

State: Powered Off
OS: Windows 10 and later x64
Version: Workstation 16.2.x virtual machine
RAM: 2 GB

10. Windows 10 installer will startup.


Windows 10 Enterprise - VMware Workstation 16 Player (Non-commercial use only)
Player
Type here to search
9:28 am
22/10/2022

11. Continue to Windows 10 setup.



Language to install: English (United States)

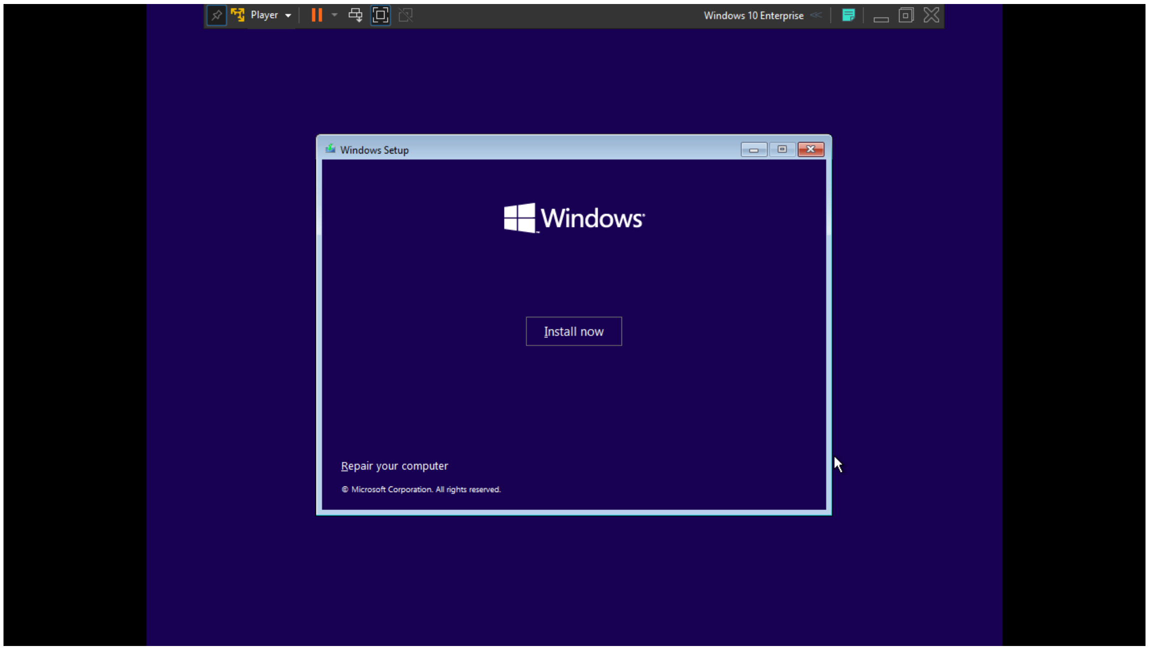
Time and currency format: English (United States)

Keyboard or input method: US

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

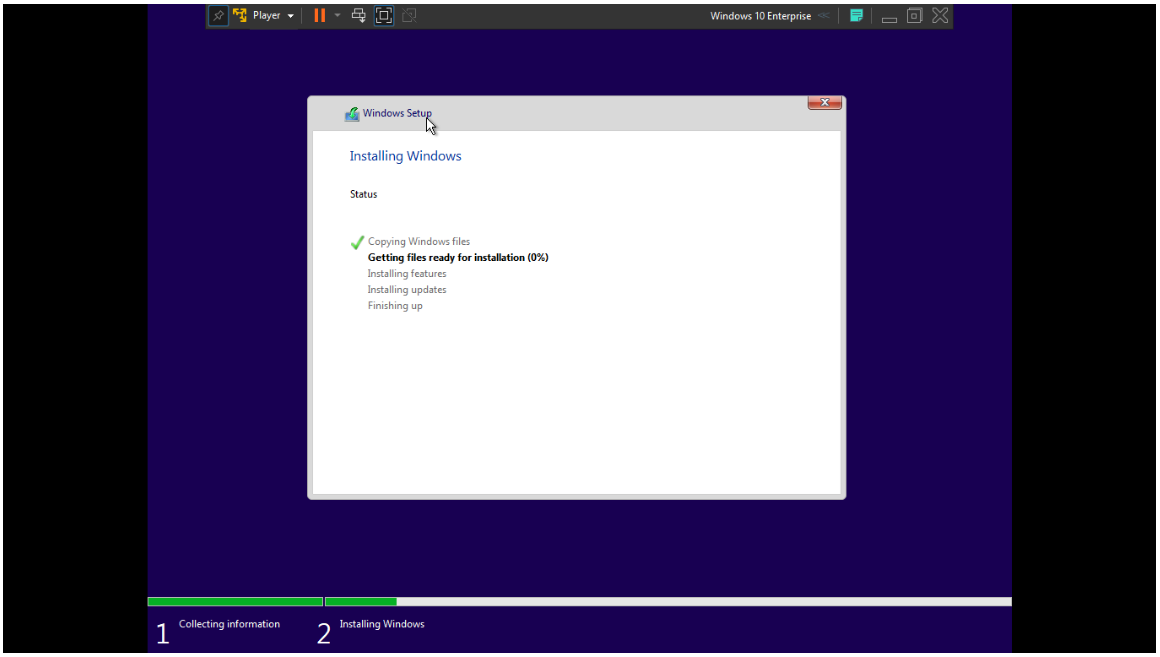
© Microsoft Corporation. All rights reserved.

12. Click Install Now.



© Microsoft Corporation. All rights reserved.

13. Go through installation process.



Windows Setup

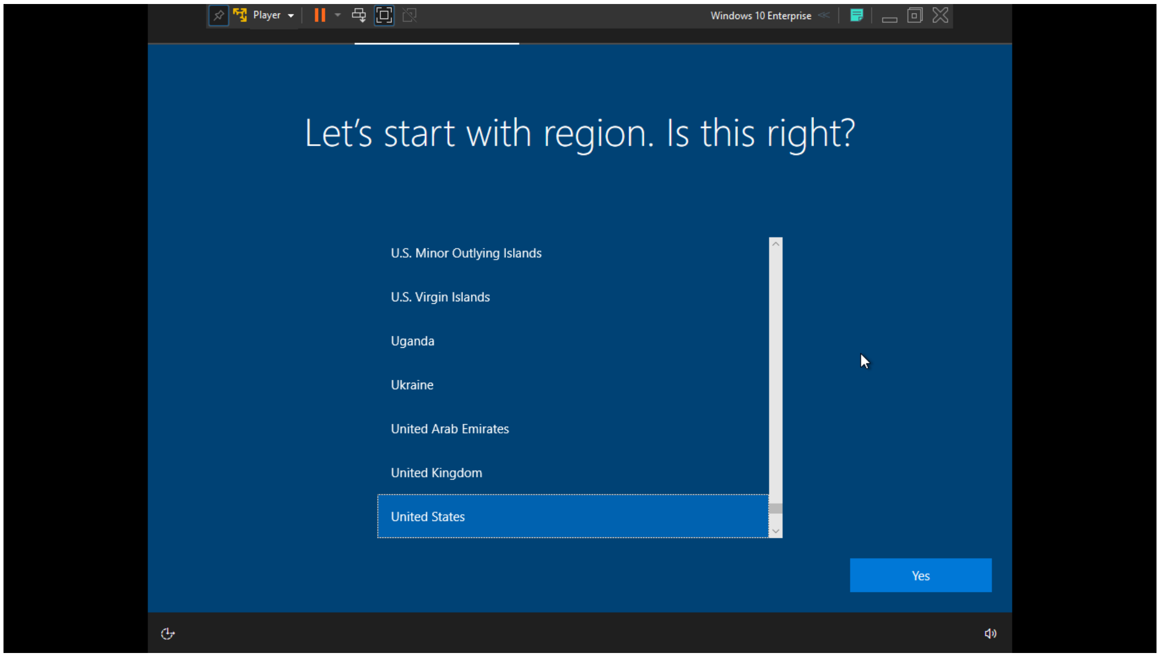
Installing Windows

Status

✓ Copying Windows files
Getting files ready for installation (0%)
Installing features
Installing updates
Finishing up

1 Collecting information
2 Installing Windows

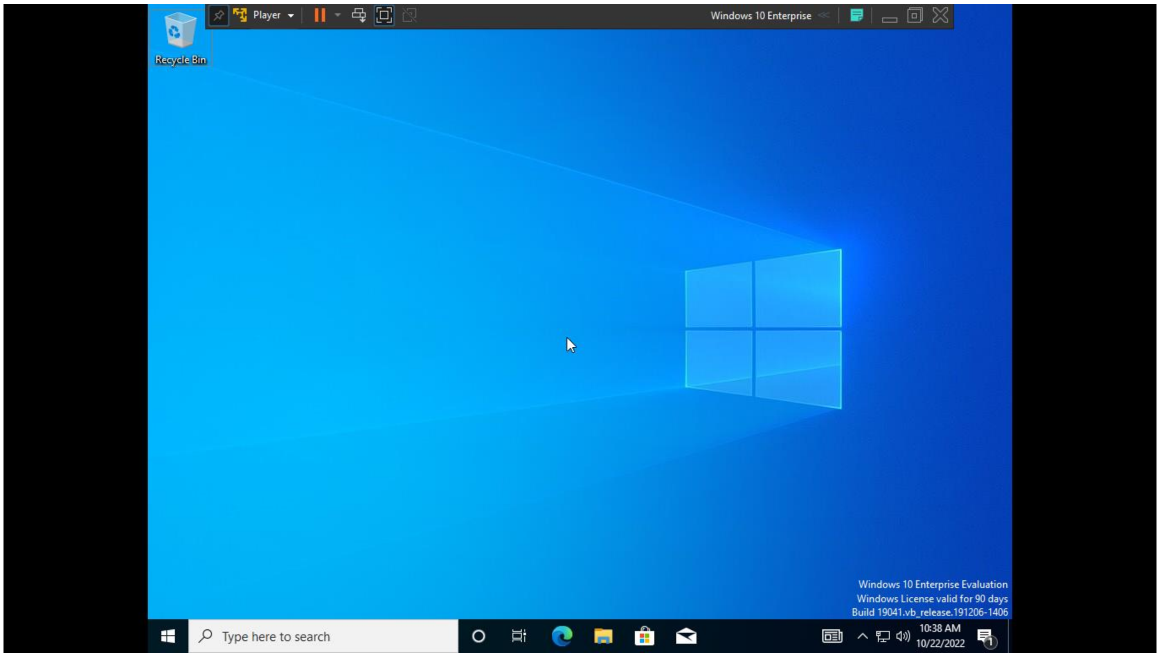
14. Go through setting up Windows 10 Operating System.



Let’s start with region. Is this right?

U.S. Minor Outlying Islands
U.S. Virgin Islands
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States

15. Windows 10 is ready for use.



Recycle Bin
Player
Windows 10 Enterprise
Windows 10 Enterprise Evaluation
Windows License valid for 90 days
Build 19041.vb_release.191206-1406
Type here to search
10:38 AM
10/22/2022

16. Close all windows.

Question 2

What are the default passwords? Why can following configuration cause serious security concerns?

1. *Default Configurations*
2. *Misconfigurations*
3. *Weak Configurations*

Why are insider attacks considered as most lethal attacks?

Some operating systems and websites provide users with default accounts having **default passwords**. These passwords are usually intended to act as a placeholder until user changes the password after initial setup. For example, Windows 10 provides users with an administrator account having a default password ‘administrator’. If left unchanged, these passwords can prove to be a security risk by acting as an attack vector for attackers.

The following configuration can cause serious security concerns,

1. Default Configuration

Many software often provide user with security features having **default configurations**. These configurations have default settings that are intended to be changed by the user. If left unchanged, these configurations can be very dangerous. Most of the time, these setting are left unchanged by the user. Users with default configurations can fall victim to digital attacks as attacker might be able to gain access to information regarding underlying operation system.

2. Misconfiguration

Misconfigurations occur when a user changes security configurations incorrectly unintentionally or intentionally. These configurations allow the device to be compromised. Misconfiguration is commonly seen in improperly configured accounts that are set up for a user that provide more access than is necessary, such as providing total access over the entire device when the access should be more limited

3. Weak Configuration

Weak configurations are very similar to misconfigurations. Instead of choosing incorrect settings, user turns off necessary security settings. This poses the same security threat as misconfigurations.

Insider attacks are considered to be most lethal form of attacks as insiders have direct access to all the resources and information within the organizations. Also, insiders have knowledge about all the possible weaknesses of an organization.

Question 3

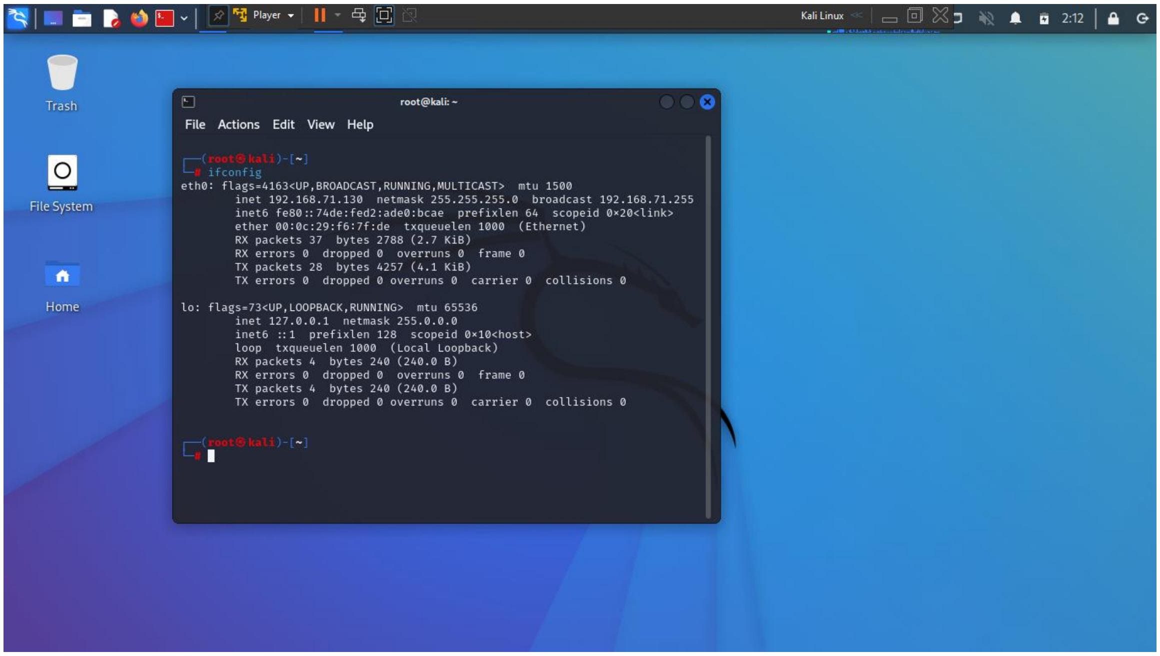
Briefly describe the functionality of following Kali Linux commands with screenshots.

Remember, you should run these commands in correct format. Elsewise, you will be marked 0.

- *Ipconfig*
- *Ping www.google.com*
- *Ping -c4 www.google.com*
- *Ping6 -c4 localhost*
- *Arp -a*
- *Tracert*
- *Nslookup*
- *Netstat*

ifconfig

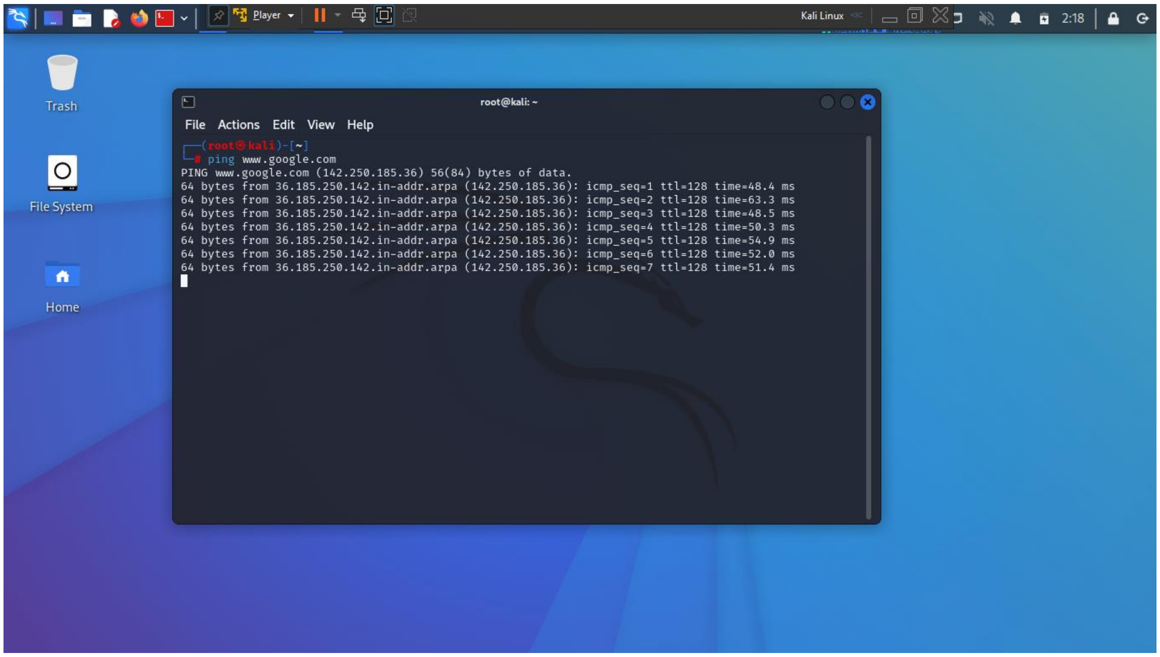
ifconfig is used to show current network interface configurations.



```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.71.130  netmask 255.255.255.0  broadcast 192.168.71.255
        inet6 fe80::74de:fed2:ade0:bcae  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:f6:7f:de  txqueuelen 1000  (Ethernet)
        RX packets 37  bytes 2788 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 4257 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# 
```

ping www.google.com

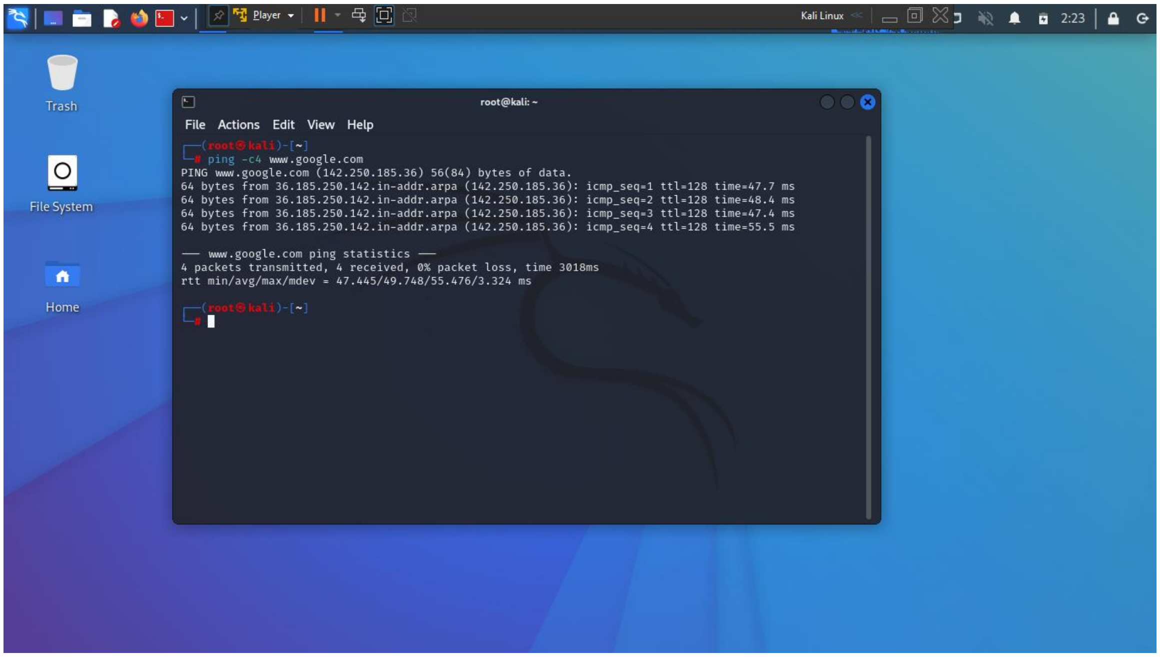
ping www.google.com is used to check connectivity between host machine and google's server.



```
┌──(root㉿kali)-[~]
└─# ping www.google.com
PING www.google.com (142.250.185.36) 56(84) bytes of data.
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=1 ttl=128 time=48.4 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=2 ttl=128 time=63.3 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=3 ttl=128 time=48.5 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=4 ttl=128 time=50.3 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=5 ttl=128 time=54.9 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=6 ttl=128 time=52.0 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=7 ttl=128 time=51.4 ms
```

ping -c4 www.google.com

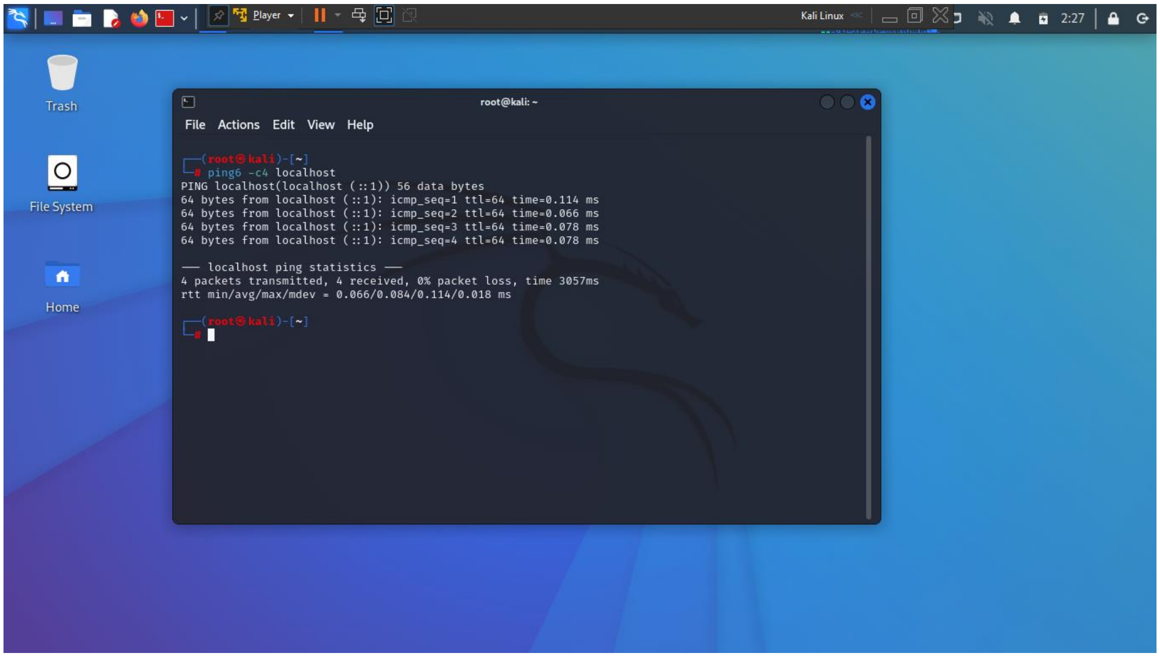
ping -c4 www.google.com is used to check connectivity between host machine and google's server using 4 packets only.



```
┌──(root㉿kali)-[~]
└─# ping -c4 www.google.com
PING www.google.com (142.250.185.36) 56(84) bytes of data.
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=1 ttl=128 time=47.7 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=2 ttl=128 time=48.4 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=3 ttl=128 time=47.4 ms
64 bytes from 36.185.250.142.in-addr.arpa (142.250.185.36): icmp_seq=4 ttl=128 time=55.5 ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 47.445/49.748/55.476/3.324 ms

┌──(root㉿kali)-[~]
└─# 
```

ping6 -c4 localhost

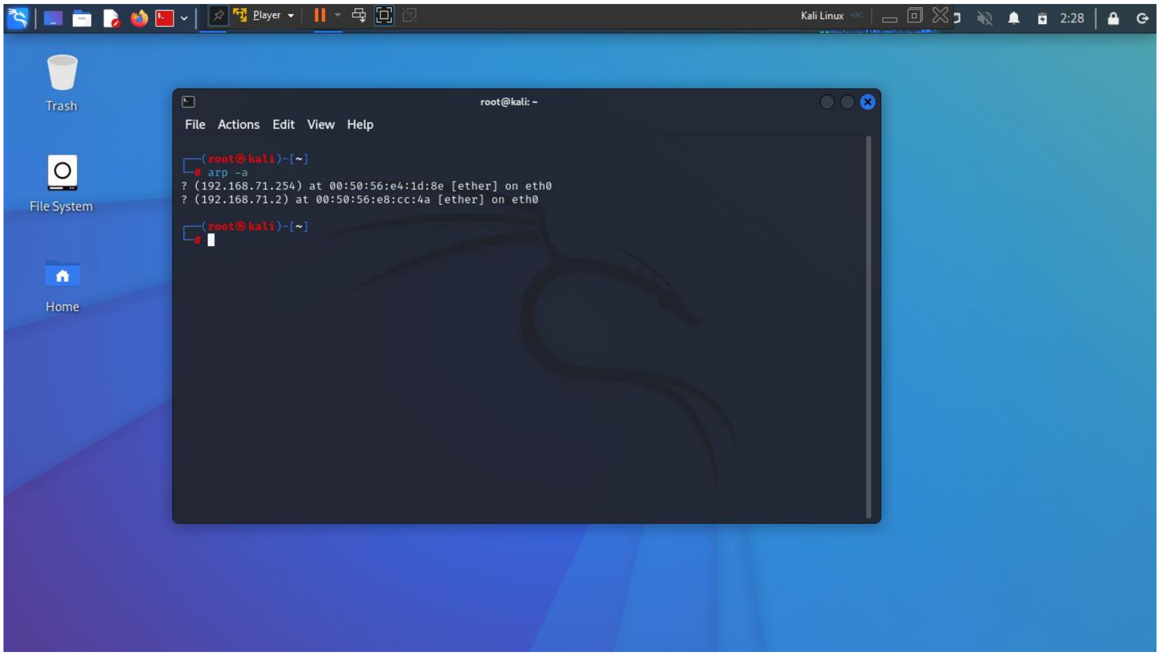
Check connectivity between localhost and host machine by sending only 4 packets.



```
┌──(root㉿kali)-[~]
└─# ping6 -c4 localhost
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.114 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.066 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.078 ms
64 bytes from localhost (::1): icmp_seq=4 ttl=64 time=0.078 ms

── localhost ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.066/0.084/0.114/0.018 ms

┌──(root㉿kali)-[~]
└─#
```

arp -a

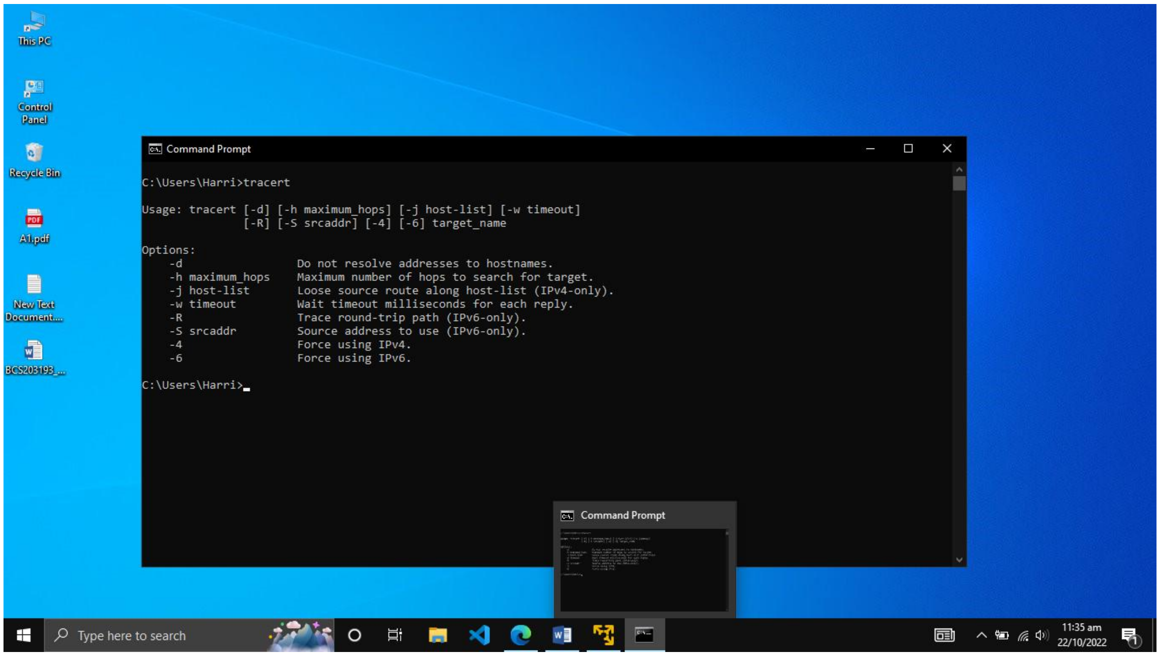
arp –a is used to display IP address, MAC address, Port and State.



```
┌──(root㉿kali)-[~]
└─# arp -a
? (192.168.71.254) at 00:50:56:e4:1d:8e [ether] on eth0
? (192.168.71.2) at 00:50:56:e8:cc:4a [ether] on eth0

┌──(root㉿kali)-[~]
└─#
```

tracert

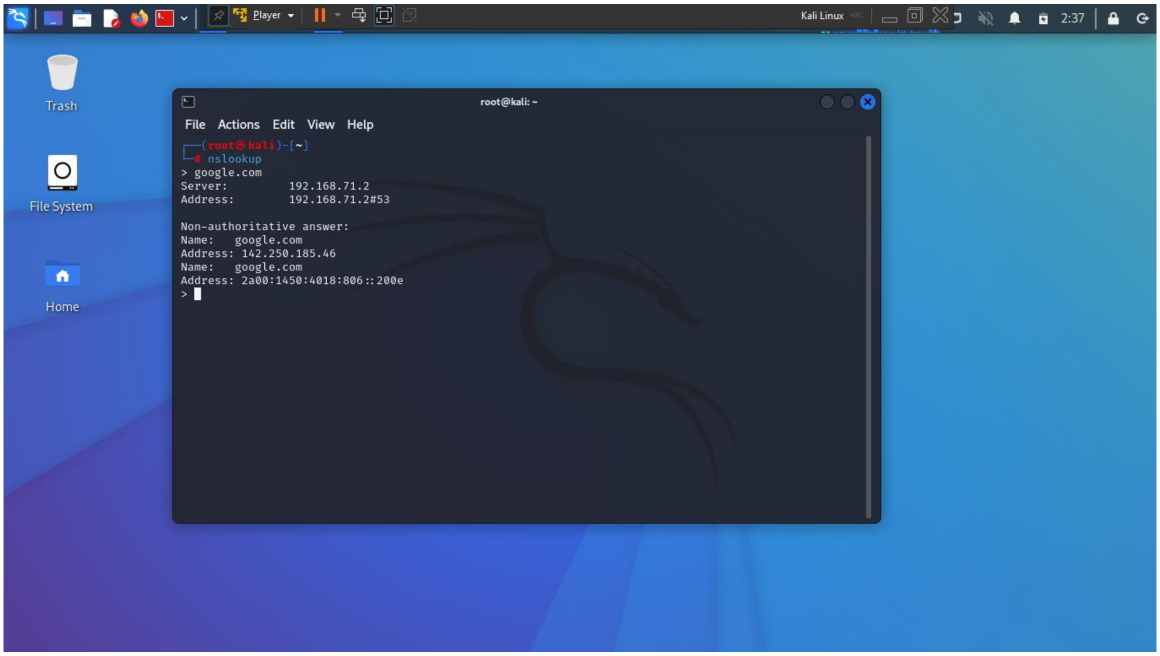
tracert is used to trace path of IP protocol.



```
C:\Users\Harri>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.

C:\Users\Harri>_
```

mslookup

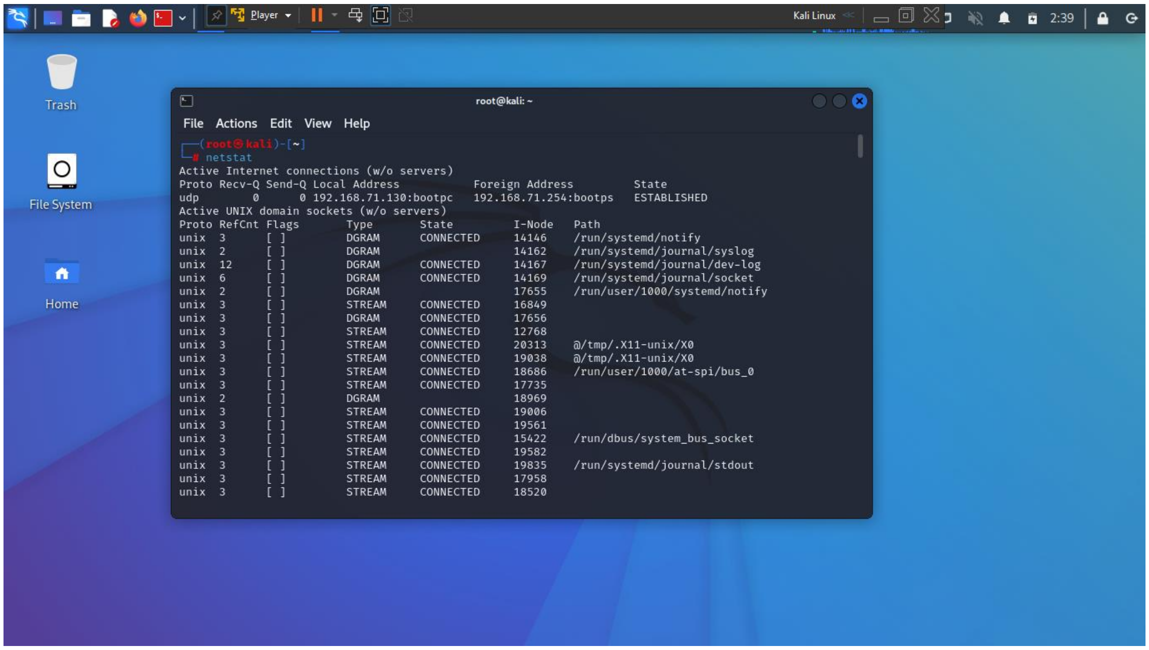
nslookup is used to display network information about destination such as IP address.



```
┌──(root㉿kali)-[~]
└─# nslookup
> google.com
Server:         192.168.71.2
Address:        192.168.71.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.185.46
Name:   google.com
Address: 2a00:1450:4018:806::200e
> █
```

netstat

netstat command displays the contents of various network-related data structures for active connections.



```
┌──(root㉿kali)-[~]
└─# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 192.168.71.130:bootpc   192.168.71.254:bootps   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         DGRAM      CONNECTED     14146    /run/systemd/notify
unix  2      [ ]         DGRAM                    14162    /run/systemd/journal/syslog
unix  12     [ ]         DGRAM      CONNECTED     14167    /run/systemd/journal/dev-log
unix  6      [ ]         DGRAM      CONNECTED     14169    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    17655    /run/user/1000/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     16849
unix  3      [ ]         DGRAM      CONNECTED     17656
unix  3      [ ]         STREAM     CONNECTED     12768
unix  3      [ ]         STREAM     CONNECTED     20313    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     19038    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     18686    /run/user/1000/at-spi/bus_0
unix  3      [ ]         STREAM     CONNECTED     17735
unix  2      [ ]         DGRAM                    18969
unix  3      [ ]         STREAM     CONNECTED     19006
unix  3      [ ]         STREAM     CONNECTED     19561
unix  3      [ ]         STREAM     CONNECTED     15422    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     19582
unix  3      [ ]         STREAM     CONNECTED     19835    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     17958
unix  3      [ ]         STREAM     CONNECTED     18520
```

References

Ciampa, M. (2018). *Comptia Security+ Guide to Network Security Fundamentals.* Boston: Cengage Learning.

Hanna, K. T. (2018, March 12). *What is default password?* Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/default-password