SIM2K
Adapting Technology to Your Business Needs

11•22
Information you can use

SIMformation

CHIPS Act – A Boost to the Economy?

The mid-term elections are now over, and we will have to see what is to come from the new faces in Congress. But one of the measures passed in the last session was the "CHIPS and Science Act of 2022," designed to move manufacturing of computer chips back to our shores. The US, where semiconductors were invented, was producing 37% of the world's supply of chips as recently as the 1990s. But only about 12% of all computer chips are produced domestically now.

That decline in domestic chip production was exposed by the worldwide supply chain crisis, and that has led to calls for reshoring microprocessor manufacturing in the US. With the federal government spurring them on, the likes of Intel, Samsung, and TSMC have unveiled plans for a flurry of new US fabrication plants. One example is chipmaker Micron Technology who announced it will spend $20 billion to build what it called the largest-ever US semiconductor factory ever, and may spend up to $100 billion over 20 years to expand it. In announcing the new fabrication plant projects, the semiconductor manufacturers, at least in part, credited the CHIPS Act, which provides $52.7 billion for manufacturing incentives to boost microchip production in the US. Chip manufacturers can begin seeking to use tax breaks and funds to offset construction and other costs beginning next year.

Essentially, the CHIPS Act is an attempt to increase the percentage of microprocessors produced in the US by closing the cost differential with other countries such as Taiwan, South Korea, and China. In those nations, the governments are already subsidizing semiconductor manufacturers. The US legislation is also meant to produce high-tech jobs and loosen the supply-chain grip foreign chip manufacturers have on US OEMs, while demonstrating that the US government is serious about supporting the industry.

The lion's share of the funding in the bill – $39 billion – goes toward incentives to build new chip foundries. There's also $2 billion for legacy chipmakers who make products critical to automotive and defense systems, $13.2 billion for research and workforce development, and $500 million for supply chain and networking security.

The question is whether that's enough. And the other issue is that once companies break ground on new manufacturing facilities, will they have access to enough tech talent to staff the facilities? Currently, the US is experiencing an unprecedented shortage of tech talent, especially in the semiconductor sector. The skills gap is exacerbating a chip supply shortage that predated supply chain disruptions caused by the COVID-19 pandemic – but the pandemic made matters worse. Older semiconductor fabrication plants were already running at maximum capacity, according to Gartner Research. "COVID exacerbated the problem because all the demand forecasting for the industry was thrown into the air," said a Gartner analyst.

Given the high costs and complexity of chip manufacturing, many US semiconductor firms transitioned to a "fabless" model, where the chips are designed here but fabricated abroad – mostly in East Asia. That region is now home to nearly 80% of global chip fabrication, according to the Center for Strategic & International Studies (CSIS). Support for re-shoring chip manufacturing was driven in large part by import shortages during the pandemic and by the dramatic increases in freight costs and delivery times. Other factors included increased recognition of the total cost of offshoring and rising concern over US dependency on China.

The potential for a Taiwan-China conflict and the danger of China interfering in the global chip supply chain have brought new focus to those concerns. "Destabilizing geopolitical and climate forces have brought to light our vulnerabilities and the need to address them," an advocacy initiative said. "Subsequently, great opportunities have arisen for a continued meaningful rebound of US manufacturing. Continuing the current trajectory will reduce the deficit, add jobs, and make the US safer, more self-reliant and resilient."

Apple, Microsoft, Alphabet, Amazon, and others have been lobbying the US government to increase domestic chip production, citing problems overseas that have hampered hardware production. In fact, a US Commerce Department report released in January said the chip shortage is so bad that at one point in 2021 there was just a five-day supply worldwide – with no sign the situation would improve anytime soon.

In contrast to the US, the governments of Taiwan, South Korea, Japan, and China all subsidize semiconductor manufacturing and research facilities, according to the Semiconductors in America Coalition (SIAC). "As a result, it is 20%-40% more expensive to build and operate a fabrication facility in the US compared to overseas," SIAC said in a letter to US Congressional leaders.

The industry feels that the government's investments to reshore chip production will create hundreds of thousands of American jobs and encourage hundreds of billions of dollars in chip company investments in the US and ensure more resilient chip supply chains for key manufacturing industries and for the national security community.

Counter-Ransomware Conference

The US White House convened its Second International Counter Ransomware Initiative Summit (CRI), bringing together leaders from 36 countries and the European Union in person to build on the work of its first ransomware summit in 2021. At a press briefing before the Summit, a White House spokesperson said, "While the United States is facilitating this meeting, we don't view this solely as a US initiative. It's an international partnership that spans most of the world's time zones, and it really reflects the threat that criminals and cyberattacks bring."

Later, the White House issued a fact sheet stating that throughout the summit, CRI and private-sector partners discussed and developed concrete, cooperative actions to counter the spread and impact of ransomware around the globe. Several common themes emerged at the summit's closing session. First, all the country participants emphasized the critical role international collaboration needs to play in defeating ransomware. The secretary of the Department of Home Affairs in Australia, said, "It's a borderless threat, so, therefore, it needs a borderless response." The national cyber security coordinator at the National Security Council Secretariat of India, said, "The exponential growth of ransomware attacks worldwide has underscored the need for global and regional cooperation in both mitigating the attacks as well as devising internationally accepted policies and procedures to attribute and disrupt the threat actors."

Another common theme of the summit is that ransomware has risen over the past five years from a petty money-making criminal enterprise to become an existential threat to all nations' social functioning and national security. Conferees agreed that ransomware is a national security imperative which can no longer be viewed as a type of organized crime carried out by non-state actors. Noting the glaring absence from the summit of Russia, which tolerates and by all accounts encourages ransomware actors within its borders, the conference stated "Cybercriminals very often act in close coordination and on behalf of states including Russia. Ransomware has become a great source of illicit profit for authoritarian regimes, and we must work together to counter this threat."

Several participants raised the need to respect that different nations have different legal authorities governing how far they can work with other countries. "We have started to think how to solve the international legal issue so we can get the attackers in cyberspace and not in legal space," said the executive director of strategy and international cooperation at Israel National Cyber Directorate.

Most of the participants say that any strategy to combat ransomware requires the participation of the private sector to succeed. An advisor to the federal chancellor at the Federal Chancellery of Austria, said that "A whole-of-society approach to delivering a deeply needed piece to solve the global ransomware puzzle needs to include predefined interfaces and cooperation with the private sector." Likewise, the digital vice minister in the Dominican Republic, said, "the government cannot achieve our cyber resilience goals alone. The private sector owns and operates much of our nation's critical infrastructure. There is only one way to defend the state from cyber threats, and that is through government industry and civil society working together, sharing appropriate information, and raising awareness and education as allies behind the same goals."

Airports Targeted by Soviet Group

Some of the nation's largest airports have been targeted for cyberattacks in mid-October by an attacker within the Russian Federation, a senior official briefed on the situation confirmed. Importantly, the systems targeted do not handle air traffic control, internal airline communications and coordination or transportation security. "It's an inconvenience," the source said.

The attacks have resulted in targeted "denial of public access" to public-facing web domains that report airport wait times and congestion. Over a dozen airport websites were impacted by the DOS attack, an intelligence analyst confirmed. That type of attack essentially overloads sites by jamming them with artificial users. "Killnet," a pro-Russian hacker group, is believed to be behind the attack. While similar groups have been found to be fronts for state-backed actors, there is no evidence the Russian government was involved in directing this attack.

The attacks were first reported around 3 a.m. ET when the Port Authority notified the Cybersecurity and Infrastructure Security Agency that the LaGuardia Airport system had been hit. LaGuardia has been restored, but other airports around the country have subsequently been targeted. The FBI and Cybersecurity and Infrastructure Security Agency, part of the Department of Homeland Security, each said they were aware of the attacks. The websites for Des Moines International Airport, Los Angeles International Airport (LAX) and Chicago O'Hare International Airport appeared impacted as well.

Later, Denver International Airport, the third busiest airport in the country, was attacked and continued to be attacked, according to an airport spokesperson. "Similar to many other U.S. airports, DEN's website has been targeted," the spokesperson said. Hartsfield-Jackson Atlanta International Airport reported around 10:30 a.m. ET that its site is back up and running and that "at no time were operations at the airport impacted."

Engineers and programmers are actively working to close backdoors that allowed the attacks and shoring up more critical computer infrastructure. Jamming attacks like the one seen Monday morning are highly visible but largely superficial and often temporary.

"We are pretty clear it's a Russian cyber group that claimed responsibility," Sen. Chuck Schumer, D-N.Y., said Monday, going on to connect the attacks to the Ukrainian bombing of a bridge in Crimea over the previous weekend.

While a DOS attack is not as impactful as a ransomware attack, which can lock down all computers and requires either payment of the ransom or extensive mitigation procedures, it is still a major incident and a reminder that proper security is essential for any network, large or small. The fact that airports were targeted is also a warning that critical infrastructure is vulnerable. Much like the attack on the Colonial Pipeline last year, and other attempts to strike at public utilities, cyber crimes may be the next front in the renews Cold War with Russia and other nations like China, Iran and North Korea.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Incognito Never was ... Incognito

A federal judge in California is considering motions to dismiss a lawsuit against Google that alleges the company misled them into believing their privacy was being protected while using Incognito mode in the Chrome browser. The lawsuit, filed in the Northern District Court of California by five users more than two years ago, is now awaiting a recent motion by those plaintiffs for two class-action certifications.

The first would cover all Chrome users with a Google account who accessed a non-Google website containing Google tracking or advertising code and who were in “Incognito mode”; the second covers all Safari, Edge, and Internet Explorer users with a Google account who accessed a non-Google website containing Google tracking or advertising code while in “private browsing mode.”

According to court documents Google employees joked about the browser’s Incognito mode and how it didn't really provide privacy; they also criticized the company for not doing more to provide users with the privacy they thought they had.

Another hearing occurred on October 11, which could have major consequences for the lawsuit. The plaintiffs’ motion for class certification was argued and they’re currently awaiting a decision, according to the law firm representing plaintiffs in the class-action suit. The Court will decide whether tens of millions of Incognito users can be grouped together to pursue statutory damages of $100 to $1,000 per violation, which could put the settlement north of $5 billion. Google also faces lawsuits related to user privacy from the Department of Justice and attorneys general in several states, including Texas, Washington, DC, and Washington state. Earlier this month, Google settled a lawsuit filed by Arizona’s AG for $85 million.

From a trust perspective, offerings like Incognito mode place users into a false sense of security as it is assumed that Incognito, and private browsing generally, will protect them from the collection of their data. When a user chooses to use Incognito mode, Google’s web browser is supposed to automatically delete browsing history and cookies at the end of a session.

The plaintiffs, who are Google account holders, alleged the search engine collected their data and distributed and sold it for targeted advertising through a real-time bidding (RTB) system.

The plaintiffs allege that even in Incognito mode, Google can see what websites Chrome users visit and collect data “through means that include Google Analytics, Google ‘fingerprinting’ techniques, concurrent Google applications and processes on a consumer’s device,” as well as Google’s AdManager. According to the lawsuit, more than 70% of all online websites “use one or more of these Google services.” Specifically, Plaintiffs allege that, whenever a user in private browsing mode visits a website that is running Google Analytics or Google Ad Manager, Google’s software scripts on the website "surreptitiously direct the user’s browser to send a secret, separate message to Google’s servers in California.” Google learns exactly what content the user’s browsing software was asking the website to display, and it also transmits a header containing the URL information of what the user has been viewing and requesting online. The device IP address, geolocation data and user ID are all tracked and recorded by Google, the lawsuit alleges.

So if you were counting on being “incognito”, think again!

“Random Tid-Bytes”

Zero-Day Apple Threat

It is recommended you immediately update your Apple devices to ward off a zero-day threat. Unfortunately, the advisory revealing this attack is somewhat sparse, and doesn't reveal a lot of information with regard to what's happening, but if you own an iPad or iPhone you should be aware of this exploit and take steps to update your operating system. Apple’s lack of detail means it’s not possible to explain what to watch out for if you think your device may have been compromised. The vulnerability affects the kernel code, the core of the software that operates the device. It can be abused to run remote code execution attacks, which can lead to issues like crashing and / or data corruption. The updates which address the above issue are iOS 15.7.1 and iPadOS 15.7.1. So be sure your devices are running these current versions.

Ransomware Scammers Tricked

Dutch police and other law enforcement agencies have managed to trick the DeadBolt ransomware operators into releasing 150 decryption keys for free. The method of obtaining decryption keys was found by a Dutch incident response company who shared the method with the police. The basis for the trick is that it was possible to cancel an unconfirmed Bitcoin transaction before payment went through, but after the decryption key was released. Because of the large amount of Bitcoin transactions taking place at one time, it can take a while for payment to actually go through. That gave police enough time to block the transactions from going through before the payment actually took place. By then they’d already received the decryption key and could pass it on to the victims. They managed to repeat the process around 150 times before the ransomware gang pulled the plug on their system that gave out the decryption keys. So sorry, not sorry, to the “bad guys.”

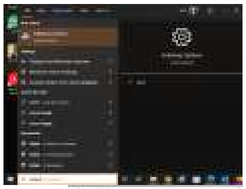
TikTok Mining Your Data

Consumer Reports (CR) has revealed that TikTok gathers data on people who don't even use the app itself. In TikTok's case, the company embeds a tracker called a “pixel.” Pixel gathers user data from these websites to help companies target ads and measure how these work. CR sought the aid of a security firm to scan for websites containing TikTok’s pixel, paying particular attention to sites that regularly deal with sensitive information, such as .gov, .org, and .edu sites. It turns out that pixels are already widespread. Among other data, TikTok collects the IP address; a unique number; the page a user is on; and what they’re clicking, typing, or searching for. While the data is used for targeted ads and ad effectiveness, a TikTok spokesperson said the data “is not used to group individuals into particular interest categories for other advertisers to target.” Data collected from non-TikTok users, however, are used in aggregated reports sent to advertisers. Most companies are unaware TikTok and other big brands gather data this way. CR noted that the only reason this works is because it’s a secret operation. “Some people might not care, but people should have a choice. It shouldn't be happening in the shadows,” the report concluded. And, given the relationship of TikTok to China, any data transfer could be problematic for national security, let alone personal security.

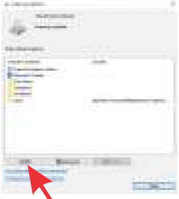
Windows 11 Search Tips

Windows Search is one of the most underused and underappreciated features of Windows simply because people just do not know how to use it productively, or worse still, just don't know that it's there. Here are tips to fully utilize this feature of Windows 11 to its full potential by performing basic searches, and how to make full use of the Advanced Query Syntax implemented by Windows Search. Before you can fully benefit from Windows Search, you first need to follow a few simple steps to configure it to your needs.

Opening Indexing Options



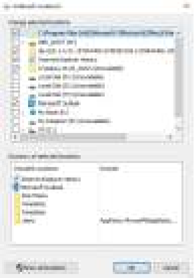
- Click the **Start** Button
- Begin typing *Index*
- Click "Indexing Options" in the search results:



The Indexing Options window shows you the status of the indexer and provides command buttons that you can use to modify the behavior of Windows Search.

The easiest way of adding a folder and all associated subfolders to the index is to add it to a Library. Sometimes, however, you want to add a drive or folder to the index, but don't want to include it in a library. So, in the Indexing Options window:

- Click the **Modify** button to open the Indexed Locations window.
- In the list of available locations, find the drive and/or folder you want to add to the index and place a check mark to select it. All subfolders are automatically selected.



- Click the boxes in the locations list to add (checked) or remove (unchecked) a drive from the index.
- If you want to exclude a specific folder, you can expand the folder list by clicking the arrows at the left of a folder name. Then remove the checkmark from the folder you want to exclude:
- When you have made the required changes to the indexed locations, click the **OK** button.

Depending on the number of files in the locations you have specified in the index, it can take anything from a few minutes to several hours to fully initialize the index:

Using Windows Search

There are two ways of searching for files on your computer - the Start Menu and Windows Explorer:

Start Menu Search

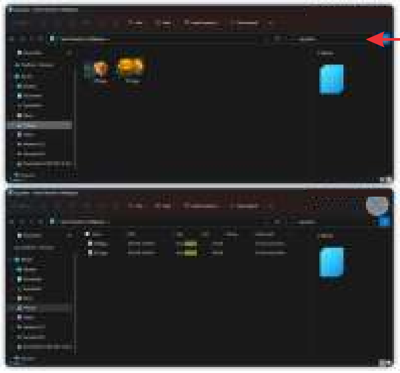
In Windows 11, the Start Menu includes a search box that can be used to search for programs, files, or the web. The most common use of which is to locate items in the Control Panel or the Start Menu itself. To use it, simply click the start button and begin typing your query. For example, to quickly find all Control Panel options relating to Networking, do the following:

- Click the Start button
- Type *network*
- You can refine your results by using the "Apps", "Document", "Web"" or "More" options of the search:
- When you have an explorer window open, pressing F3 will shift input focus to the search bar where you can immediately start typing.

By default, both the Start Menu search and Explorer Search limits itself to results pertaining to filenames only. This can be frustrating and often does not give you the results you are looking for.

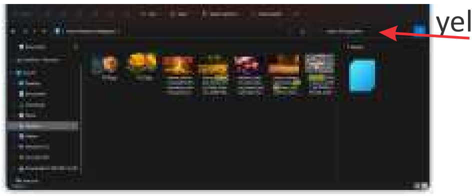
The solution is to search use the TAG: operator to further refine the search:

You can change the view from Thumbnail to Details Ctrl + Shift + 6, You'll now see that Explorer has indeed located the results from the embedded tags.



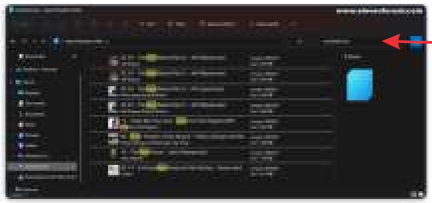
tag:yellow

But now the files returned in my initial search are not there! So how do I have Explorer return results that both match the filename and the tags? Combine your search with the Boolean OR operator, which must be typed in UPPERCASE to be recognized as such:



yellow OR tag:yellow

Now, what happens if your search results contain multiple file types? You need a way to filter down the results to find what you want. In the search below of "Red", we only want to see music. To do that, use the KIND: operator to restrict search results to music files only:

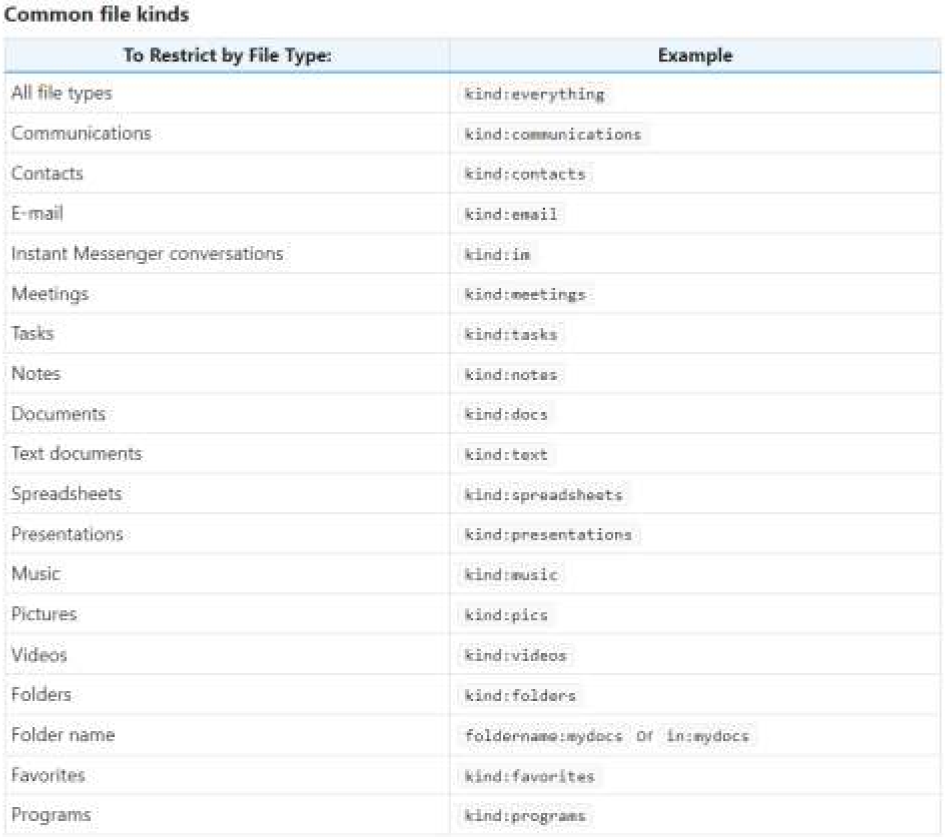


red KIND:music

You can utilize Advanced Query Syntax to help you quickly define and narrow your searches for even more targeted results.You can narrow your searches using a variety of keywords, or search parameters, which can restrict your query to specific locations, specific file types or properties within those types, or specific "file kinds". The tables on the next pages give you an overview of additional syntax, including the properties that can be added to your search terms to narrow and refine your results.

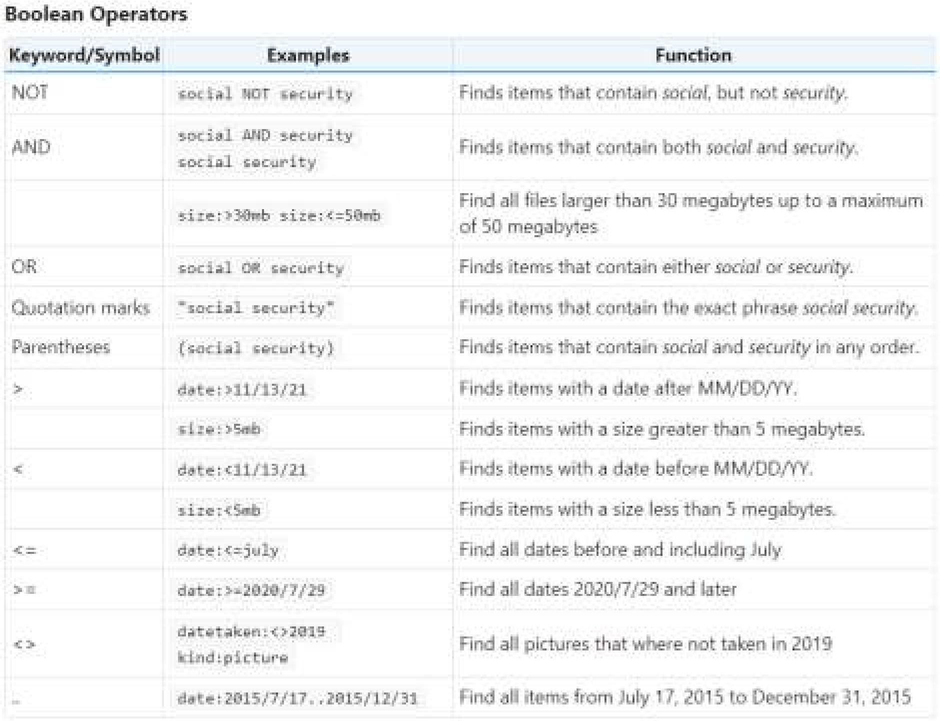
Windows 11 Search Terms and Syntax

Here are some of the phrases and search suggestions you can save and use to help make your searches more on-target and productice:



Common file kinds

To Restrict by File Type:	Example
All file types	`kind:everything`
Communications	`kind:communications`
Contacts	`kind:contacts`
E-mail	`kind:email`
Instant Messenger conversations	`kind:im`
Meetings	`kind:meetings`
Tasks	`kind:tasks`
Notes	`kind:notes`
Documents	`kind:docs`
Text documents	`kind:text`
Spreadsheets	`kind:spreadsheets`
Presentations	`kind:presentations`
Music	`kind:music`
Pictures	`kind:pics`
Videos	`kind:videos`
Folders	`kind:folders`
Folder name	`foldername:mydocs` or `in:mydocs`
Favorites	`kind:favorites`
Programs	`kind:programs`



Boolean Operators

Keyword/Symbol	Examples	Function
NOT	`social NOT security`	Finds items that contain *social*, but not *security*.

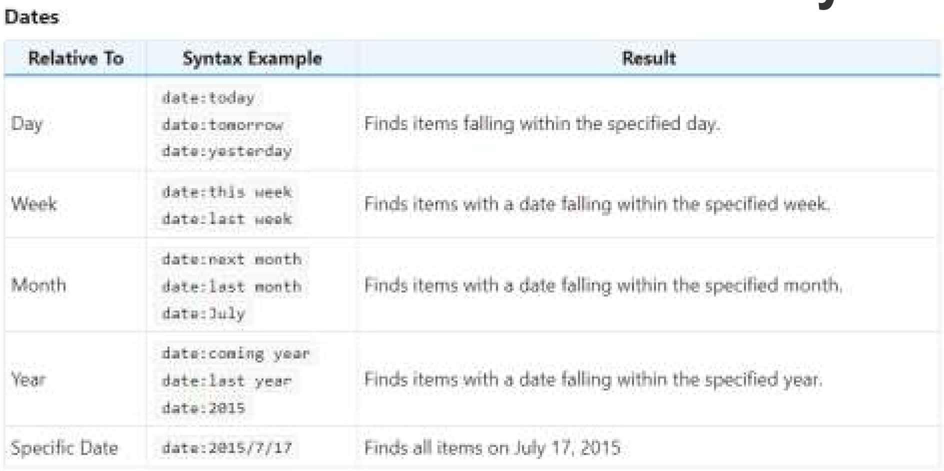
AND	`social AND security`
	`social security`
		Finds items that contain both *social* and *security*.

	`size:>30mb size:<=50mb`	Find all files larger than 30 megabytes up to a maximum of 50 megabytes
OR	`social OR security`	Finds items that contain either *social* or *security*.
Quotation marks	`"social security"`	Finds items that contain the exact phrase *social security*.
Parentheses	`(social security)`	Finds items that contain *social* and *security* in any order.
>	`date:>11/13/21`	Finds items with a date after MM/DD/YY.
	`size:>5mb`	Finds items with a size greater than 5 megabytes.
<	`date:<11/13/21`	Finds items with a date before MM/DD/YY.
	`size:<5mb`	Finds items with a size less than 5 megabytes.
<=	`date:<=july`	Find all dates before and including July
>=	`date:>=2020/7/29`	Find all dates 2020/7/29 and later

<>	`datetaken:<>2019`
	`kind:picture`
		Find all pictures that where not taken in 2019

..	`date:2015/7/17..2015/12/31`	Find all items from July 17, 2015 to December 31, 2015

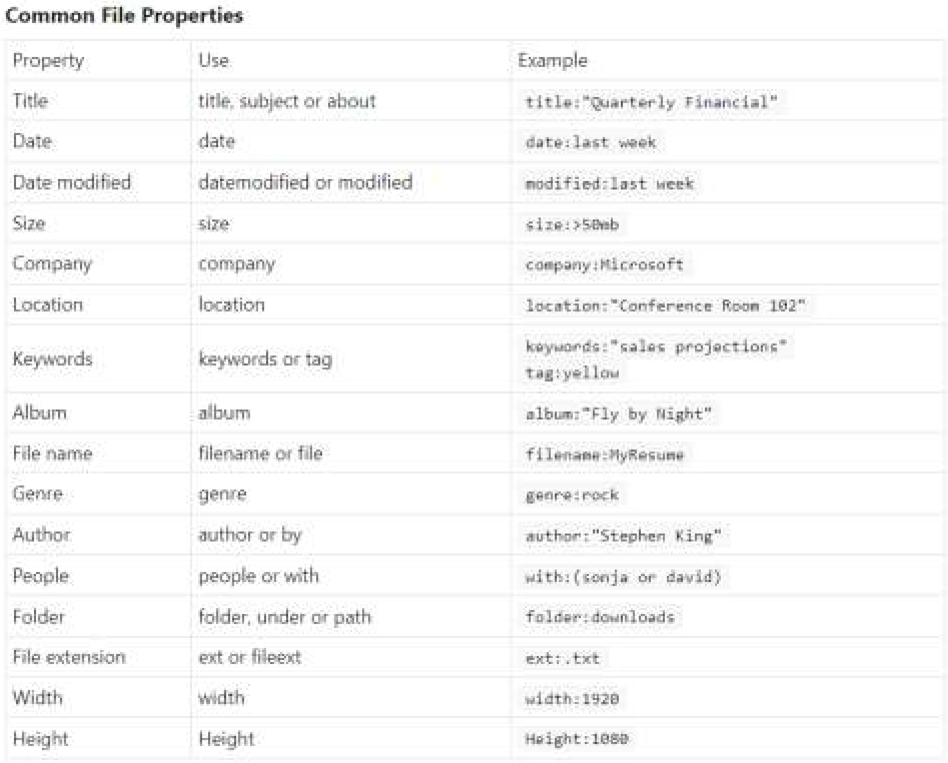
Windows 11 Search Terms and Syntax



Dates

Relative To	Syntax Example	Result
Day	date:today date:tomorrow date:yesterday	Finds items falling within the specified day.
Week	date:this week date:last week	Finds items with a date falling within the specified week.
Month	date:next month date:last month date:July	Finds items with a date falling within the specified month.
Year	date:coming year date:last year date:2015	Finds items with a date falling within the specified year.
Specific Date	date:2015/7/17	Finds all items on July 17, 2015

NOTE: When using the date: specifier, Windows Search uses the date the file or item was created.

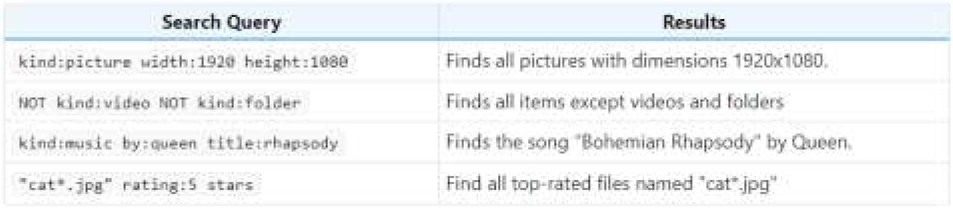


Common File Properties

Property	Use	Example
Title	title, subject or about	title:"Quarterly Financial"
Date	date	date:last week
Date modified	datemodified or modified	modified:last week
Size	size	size:>50mb
Company	company	company:Microsoft
Location	location	location:"Conference Room 102"
Keywords	keywords or tag	keywords:"sales projections" tag:yellow
Album	album	album:"Fly by Night"
File name	filename or file	filename:MyResume
Genre	genre	genre:rock
Author	author or by	author:"Stephen King"
People	people or with	with:(sonja or david)
Folder	folder, under or path	folder:downloads
File extension	ext or fileext	ext:.txt
Width	width	width:1920
Height	Height	Height:1080

Compound Search

You can easily combine any of the above operators to create compound searches to quickly find exactly what you are looking for. Examples are:



Search Query	Results
kind:picture width:1920 height:1080	Finds all pictures with dimensions 1920x1080.
NOT kind:video NOT kind:folder	Finds all items except videos and folders
kind:music by:queen title:rhapsody	Finds the song "Bohemian Rhapsody" by Queen.
"cat*.jpg" rating:5 stars	Find all top-rated files named "cat*.jpg"