Security 1
Layers

Exposures – what can you lose

- Identity, accounts
- Privacy, data
- Dollars
- Functionality
- Communication ability
- Time

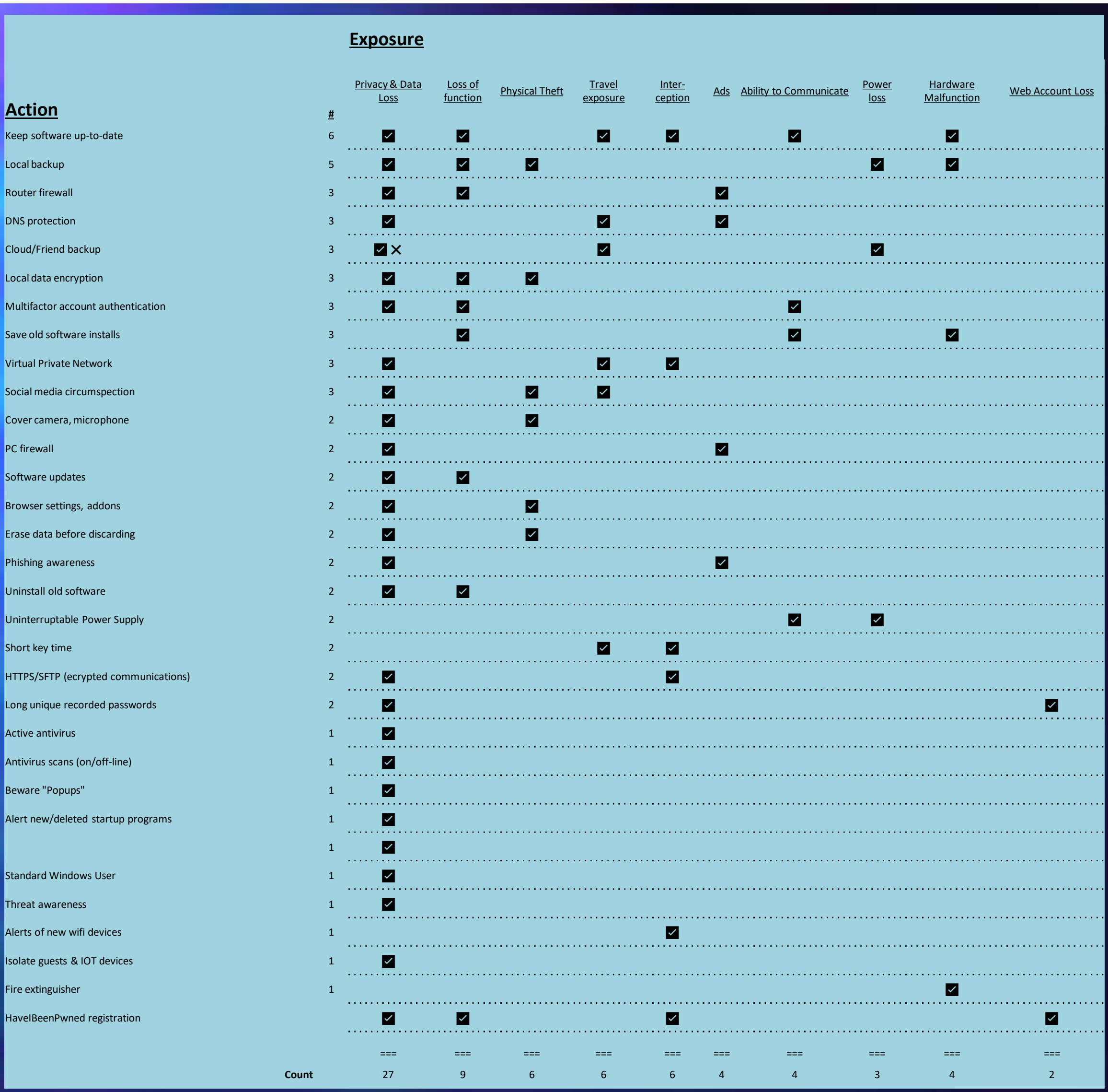
Privacy, data

- Documents
- Photographs
- Video
- Email, chat
- Programs

Who/what are the threats?

- Hardware malfunction
- Fire, flood, theft
- Power glitches/failure
- Internet thieves/vandals
- State actors – vs. journalists, protestors
  - *Need extreme security!!*

Action matrix



		Exposure									
Action	#	Privacy & Data Loss	Loss of function	Physical Theft	Travel exposure	Inter-ception	Ads	Ability to Communicate	Power loss	Hardware Malfunction	Web Account Loss
Keep software up-to-date	6	☑	☑		☑	☑		☑		☑	
Local backup	5	☑	☑	☑					☑	☑	
Router firewall	3	☑	☑				☑				
DNS protection	3	☑			☑		☑				
Cloud/Friend backup	3	☑ ✕			☑				☑		
Local data encryption	3	☑	☑	☑							
Multifactor account authentication	3	☑	☑					☑			
Save old software installs	3		☑					☑		☑	
Virtual Private Network	3	☑			☑	☑					
Social media circumspection	3	☑		☑	☑						
Cover camera, microphone	2	☑		☑							
PC firewall	2	☑					☑				
Software updates	2	☑	☑								
Browser settings, addons	2	☑		☑							
Erase data before discarding	2	☑		☑							
Phishing awareness	2	☑					☑				
Uninstall old software	2	☑	☑								
Uninterruptable Power Supply	2							☑	☑		
Short key time	2				☑	☑					
HTTPS/SFTP (ecrypted communications)	2	☑				☑					
Long unique recorded passwords	2	☑									☑
Active antivirus	1	☑									
Antivirus scans (on/off-line)	1	☑									
Beware "Popups"	1	☑									
Alert new/deleted startup programs	1	☑									
	1	☑									
Standard Windows User	1	☑									
Threat awareness	1	☑									
Alerts of new wifi devices	1					☑					
Isolate guests & IOT devices	1	☑									
Fire extinguisher	1									☑	
HaveIBeenPwned registration		☑	☑			☑					☑
		===	===	===	===	===	===	===	===	===	===
Count		27	9	6	6	6	4	4	3	4	2

Act to avoid or mitigate damage

- Encrypt data, communications
- Backup data, programs hardware
- Authenticate user
- Prevent problems
- Detect problems & correct

Encrypt Disks

- Hardware – Set password in BIOS
- Veracrypt (Win, Mac, Linux)
  - https://www.veracrypt.fr/code/VeraCrypt/
- Windows

Windows

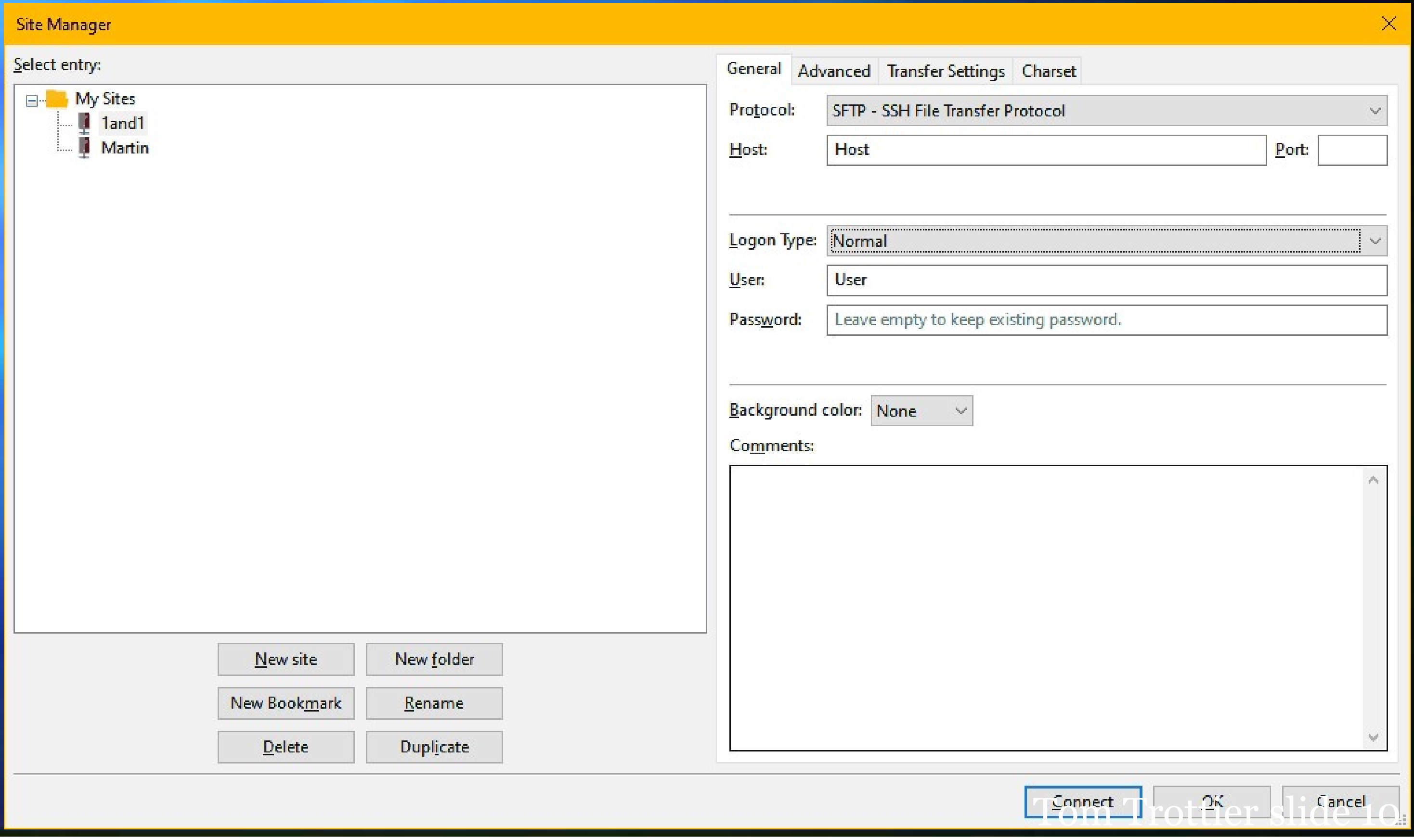
- "Device Encryption"
  - https://www.howtogeek.com/234826/how-to-enable-full-disk-encryption-on-windows-10/
  - Requires MS account, PC support
    - *Can recover encryption key from MS*
  - Often default on some PCs, e.g. ASUS T100
- Bitlocker (in Windows Pro)

Encrypt Communications

- No guarantee of other end identity – that’s Authentication
- **HTTPS - Hypertext Transfer Protocol Secure**
- **SFTP – Secure File Transfer Protocol**

SFTP – Secure File Transfer Protocol

- E.g. Filezilla



Site Manager

Select entry:

- My Sites
  - 1and1
  - Martin

General | Advanced | Transfer Settings | Charset

Protocol: SFTP - SSH File Transfer Protocol

Host: Host   Port:

Logon Type: Normal

User: User

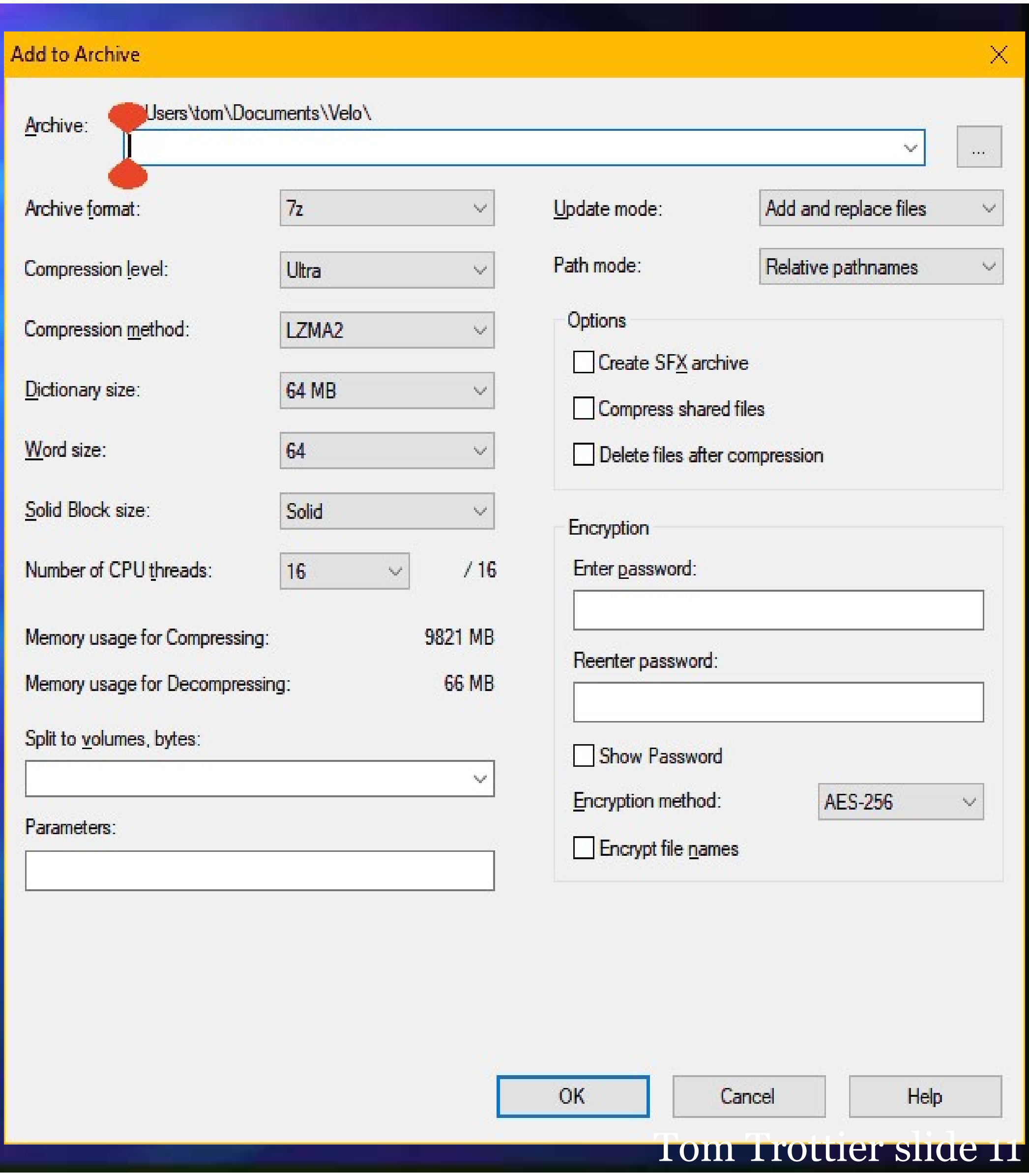
Password: Leave empty to keep existing password.

Background color: None

Comments:

Encrypt Files

- 7-zip offers archive encryption with compression



Add to Archive

Archive: Users\tom\Documents\Velo\

Archive format: 7z

Compression level: Ultra

Compression method: LZMA2

Dictionary size: 64 MB

Word size: 64

Solid Block size: Solid

Number of CPU threads: 16 / 16

Memory usage for Compressing: 9821 MB

Memory usage for Decompressing: 66 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

Enter password:

Reenter password:

□ Show Password

Encryption method: AES-256

□ Encrypt file names

Backup

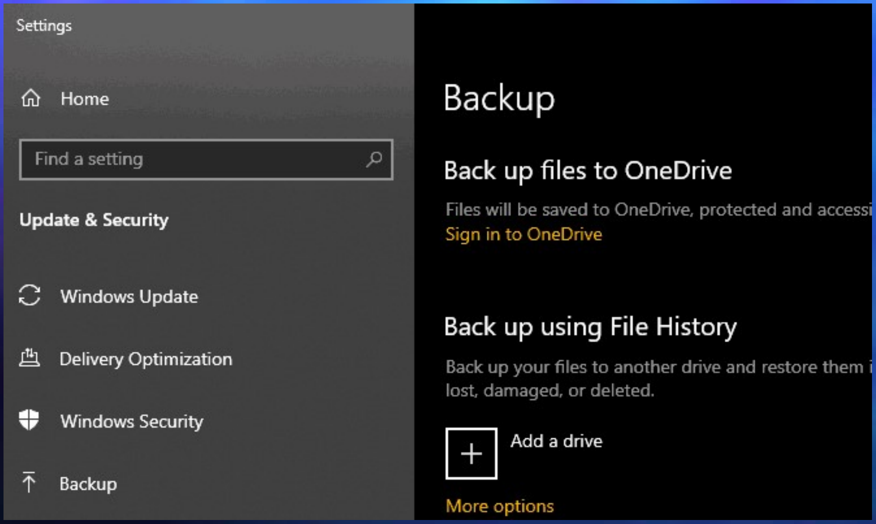
- Keep original/previous program install CDs/DVDs/ZIPs/MSIs/EXEs
- Hardware – extra/old cables, disks, routers, PCs in case of failure & immediate need
  - For devices, need to keep software current
- PC Account
  - Have backup Admin account

Data, programs

- Cloud backup, e.g., https://www.backblaze.com/ Google, Dropbox, Onedrive
- Local attached storage
  - Network attached(NAS) – available to all devices, e.g., phone, TV
  - USB attached (3, 3.1, 3.2 is faster than gigabit NAS)
    - *Might avoid ransomware by attaching only when backing up*
- Backup Software

Backup Software

- https://opcug.ca/Reviews/EaseUSBackup65.htm
- **Windows -** ***File History - OS system disk image***



Backup

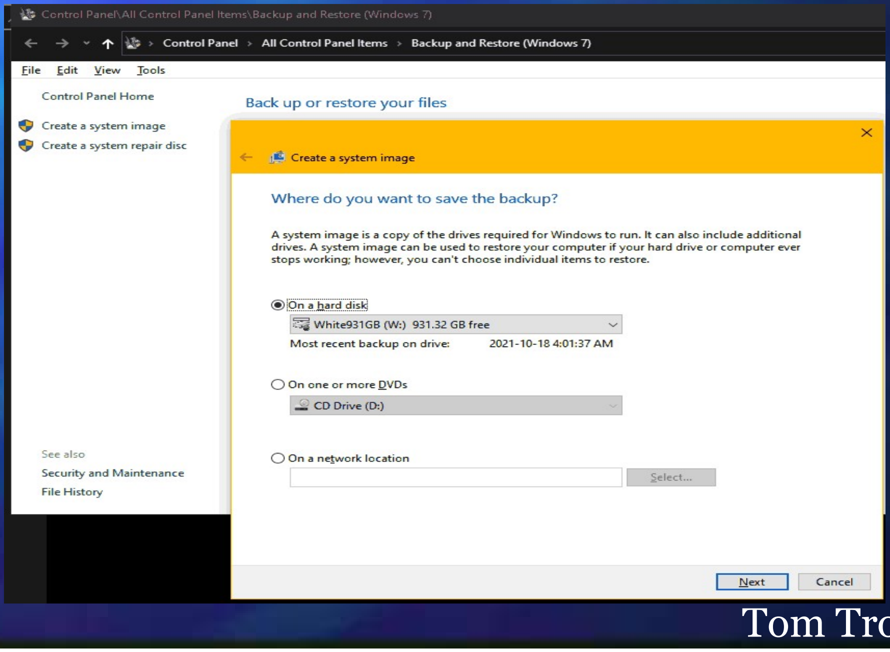
Back up files to OneDrive

Files will be saved to OneDrive, protected and accessi

Sign in to OneDrive

Back up using File History

Back up your files to another drive and restore them i
lost, damaged, or deleted.



Back up or restore your files

Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

● On a hard disk

White931GB (W:) 931.32 GB free

Most recent backup on drive: 2021-10-18 4:01:37 AM

○ On one or more DVDs

CD Drive (D:)

○ On a network location

Authentication – who are you?

- Passwords
  - PC, Disk – can set in bios
  - Windows
    - *21 characters plus to avoid Rainbow tables discovery*
  - Password manager - PC, phone, tablet
    - Lastpass, 1pass
    - https://keepass.info/
- **Multifactor**

Multifactor - something you:

- Have, e.g. “key”
  - FIDO2(USB/bluetooth/NFC “key”), bank card, …
- Know
  - Password, pass-phrase, PIN,…
- Are
  - Fingerprint, face, retina, voice, iris,…
- Can do
  - Recognize Amazon obfuscated characters, reCaptcha images,…
- Fit
  - Location, connection, network, software,…

Prevention

- Circumspect social awareness posts
  - Avoid telling world you are on vacation!
- Fire extinguisher for “class C” (electrical) fires
  - https://wiki.ezvid.com/best-fire-extinguishers
- Careful power, wire management
- Surge suppressors to manage lightning surges
- For floods, plans (attic, sand bags,…)
- Use standard account ordinarily, administrator account for installs
- Virus/privacy filter , firewall
- Uninterruptable Power Supply - for graceful PC, NAS shutdown
- Your network awareness -

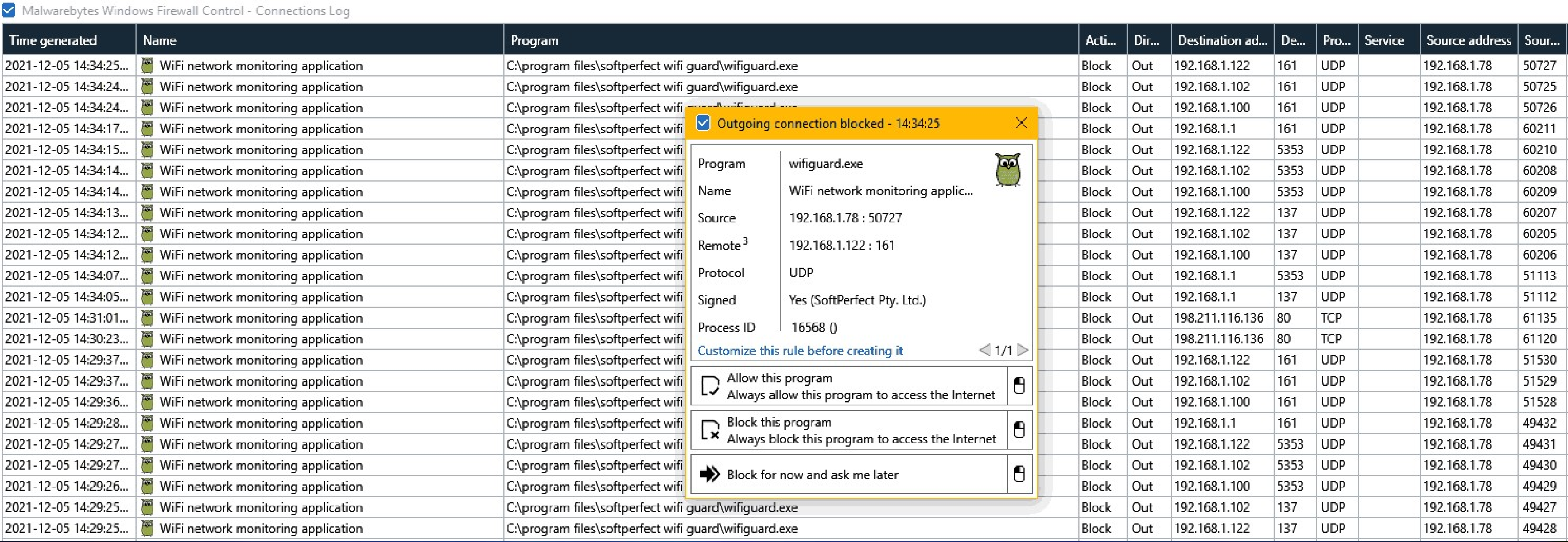
Uninterruptable Power Supply

- Gives 10-15 minutes
  for graceful PC, NAS shutdown
- Plus generator if power failures common
- Data Centres are usually put on the boundary of two power grids & tied to both to avoid shutting down if one fails.

Windows Firewall Control

- https://www.binisoft.org/wfc.php
- Nicer interface to Windows Firewall
- Alerts about new accesses
- Create, delete edit firewall rules

Firewall alerts



☑ Malwarebytes Windows Firewall Control - Connections Log

Time generated	Name	Program	Acti...	Dir...	Destination ad...	De...	Pro...	Service	Source address	Sour...
2021-12-05 14:34:25...	WiFi network monitoring application	C:\program files\softperfect wifi guard\wifiguard.exe	Block	Out	192.168.1.122	161	UDP		192.168.1.78	50727
2021-12-05 14:34:24...	WiFi network monitoring application	C:\program files\softperfect wifi guard\wifiguard.exe	Block	Out	192.168.1.102	161	UDP		192.168.1.78	50725
2021-12-05 14:34:24...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.100	161	UDP		192.168.1.78	50726
2021-12-05 14:34:17...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.1	161	UDP		192.168.1.78	60211
2021-12-05 14:34:15...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.122	5353	UDP		192.168.1.78	60210
2021-12-05 14:34:14...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.102	5353	UDP		192.168.1.78	60208
2021-12-05 14:34:14...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.100	5353	UDP		192.168.1.78	60209
2021-12-05 14:34:13...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.122	137	UDP		192.168.1.78	60207
2021-12-05 14:34:12...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.102	137	UDP		192.168.1.78	60205
2021-12-05 14:34:12...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.100	137	UDP		192.168.1.78	60206
2021-12-05 14:34:07...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.1	5353	UDP		192.168.1.78	51113
2021-12-05 14:34:05...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.1	137	UDP		192.168.1.78	51112
2021-12-05 14:31:01...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	198.211.116.136	80	TCP		192.168.1.78	61135
2021-12-05 14:30:23...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	198.211.116.136	80	TCP		192.168.1.78	61120
2021-12-05 14:29:37...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.122	161	UDP		192.168.1.78	51530
2021-12-05 14:29:37...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.102	161	UDP		192.168.1.78	51529
2021-12-05 14:29:36...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.100	161	UDP		192.168.1.78	51528
2021-12-05 14:29:28...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.1	161	UDP		192.168.1.78	49432
2021-12-05 14:29:27...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.122	5353	UDP		192.168.1.78	49431
2021-12-05 14:29:27...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.102	5353	UDP		192.168.1.78	49430
2021-12-05 14:29:26...	WiFi network monitoring application	C:\program files\softperfect wifi	Block	Out	192.168.1.100	5353	UDP		192.168.1.78	49429
2021-12-05 14:29:25...	WiFi network monitoring application	C:\program files\softperfect wifi guard\wifiguard.exe	Block	Out	192.168.1.102	137	UDP		192.168.1.78	49427
2021-12-05 14:29:25...	WiFi network monitoring application	C:\program files\softperfect wifi guard\wifiguard.exe	Block	Out	192.168.1.122	137	UDP		192.168.1.78	49428

☑ Outgoing connection blocked - 14:34:25

Program	wifiguard.exe
Name	WiFi network monitoring applic...
Source	192.168.1.78 : 50727
Remote[3]	192.168.1.122 : 161
Protocol	UDP
Signed	Yes (SoftPerfect Pty. Ltd.)
Process ID	16568 ()

Customize this rule before creating it   1/1

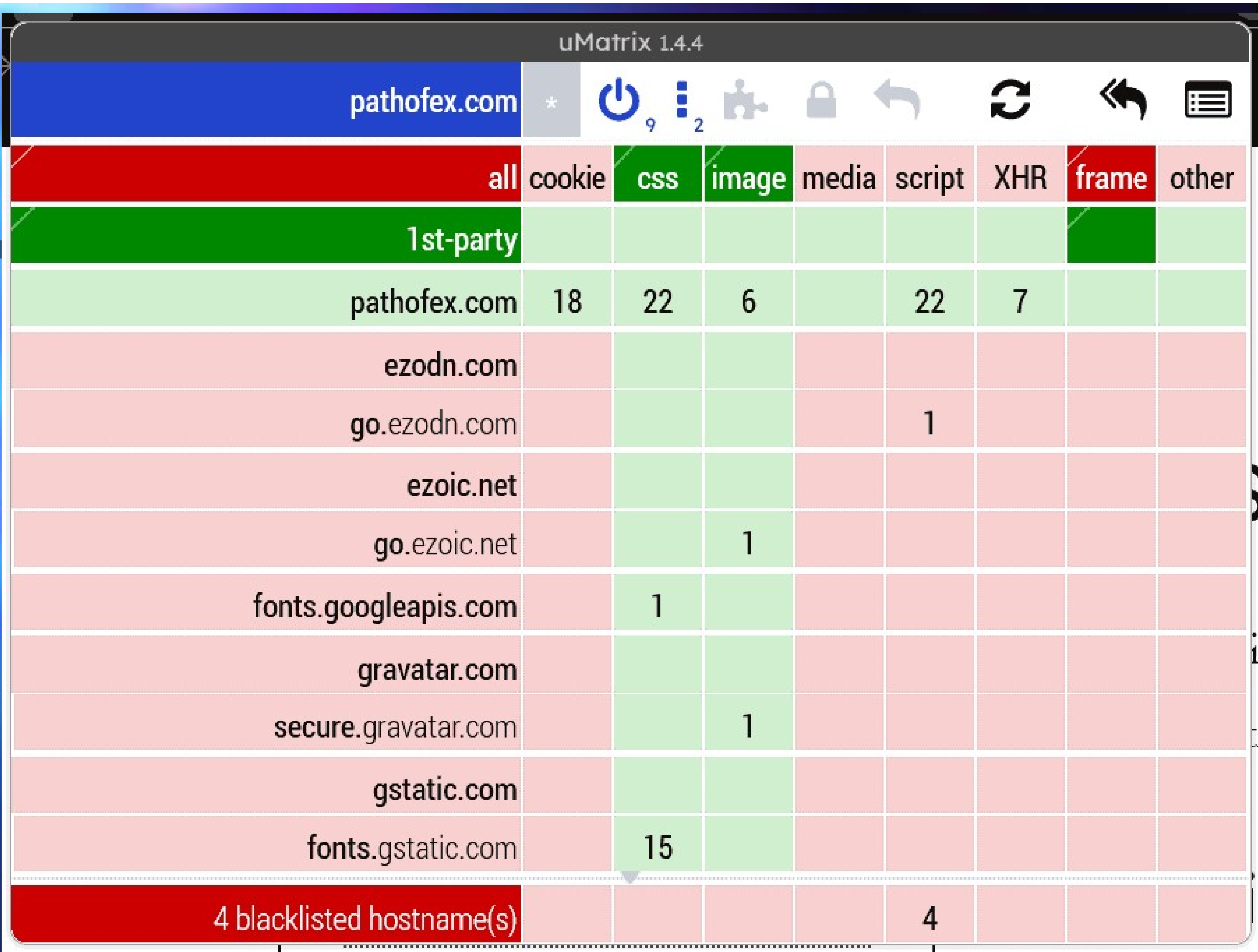
Allow this program
Always allow this program to access the Internet
Block this program
Always block this program to access the Internet
Block for now and ask me later

Virus/privacy filter

- Windows “Security” very good
- Windows Firewall good
- Browser add-ons
  - Umatrix
  - Ublock origin
  - Privacy badger

Umatrix

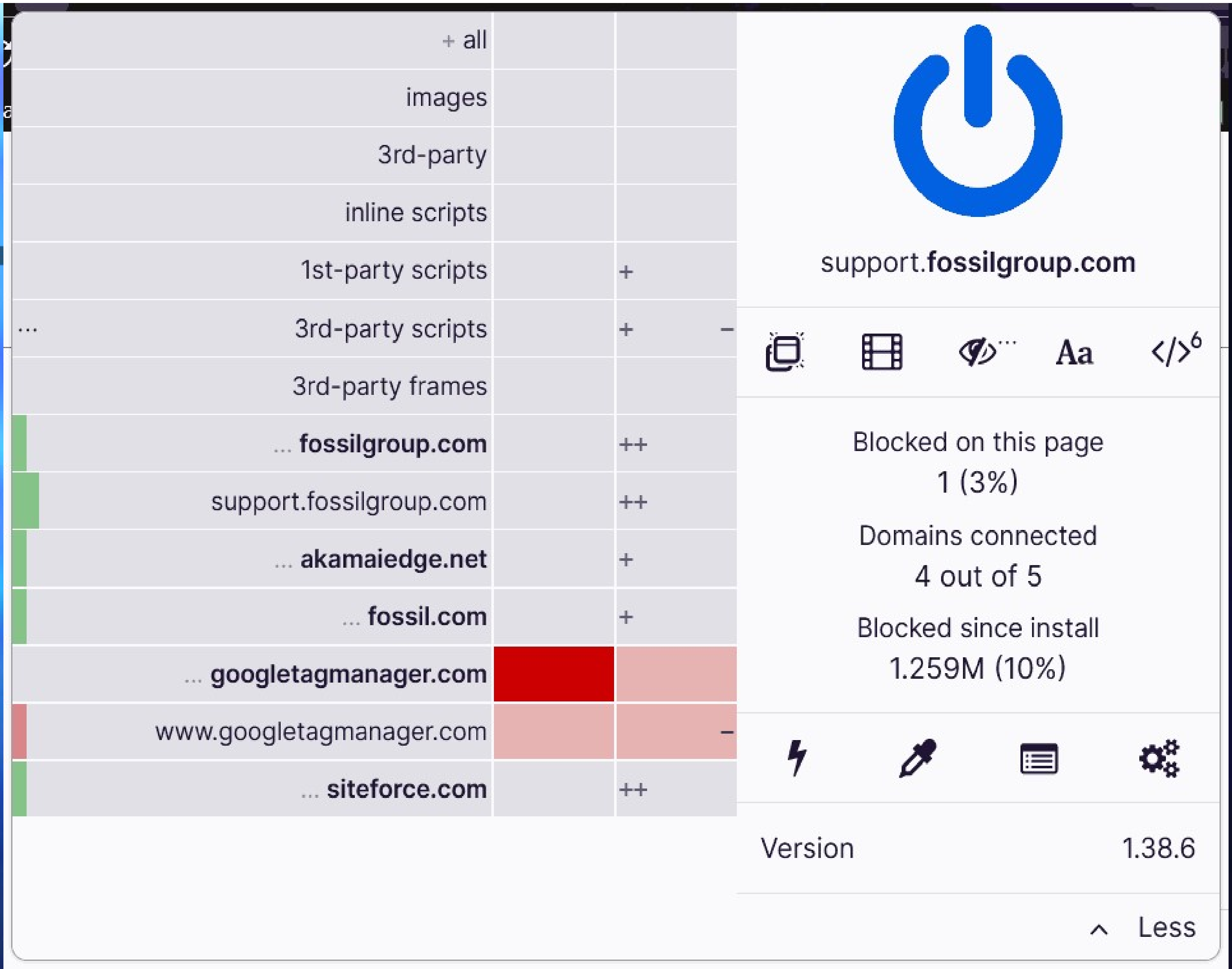
- Add-on (extension) for most browsers
- Can click boxes/lines to allow/ disallow



all	cookie	css	image	media	script	XHR	frame	other
1st-party								
pathofex.com	18	22	6		22	7		
ezodn.com								
go.ezodn.com					1			
ezoic.net								
go.ezoic.net			1					
fonts.googleapis.com		1						
gravatar.com								
secure.gravatar.com			1					
gstatic.com								
fonts.gstatic.com		15						
4 blacklisted hostname(s)					4			

Ublock origin

- Add-on (extension) for most browsers
- Can click boxes/lines to allow/ disallow



+ all		
images		
3rd-party		
inline scripts		
1st-party scripts		+
... 3rd-party scripts		+ −
3rd-party frames		
... **fossilgroup.com**		++
support.fossilgroup.com		++
... **akamaiedge.net**		+
... **fossil.com**		+
... **googletagmanager.com**	🟥	🟥
www.googletagmanager.com	🟥	🟥 −
... **siteforce.com**		++

support.**fossilgroup.com**

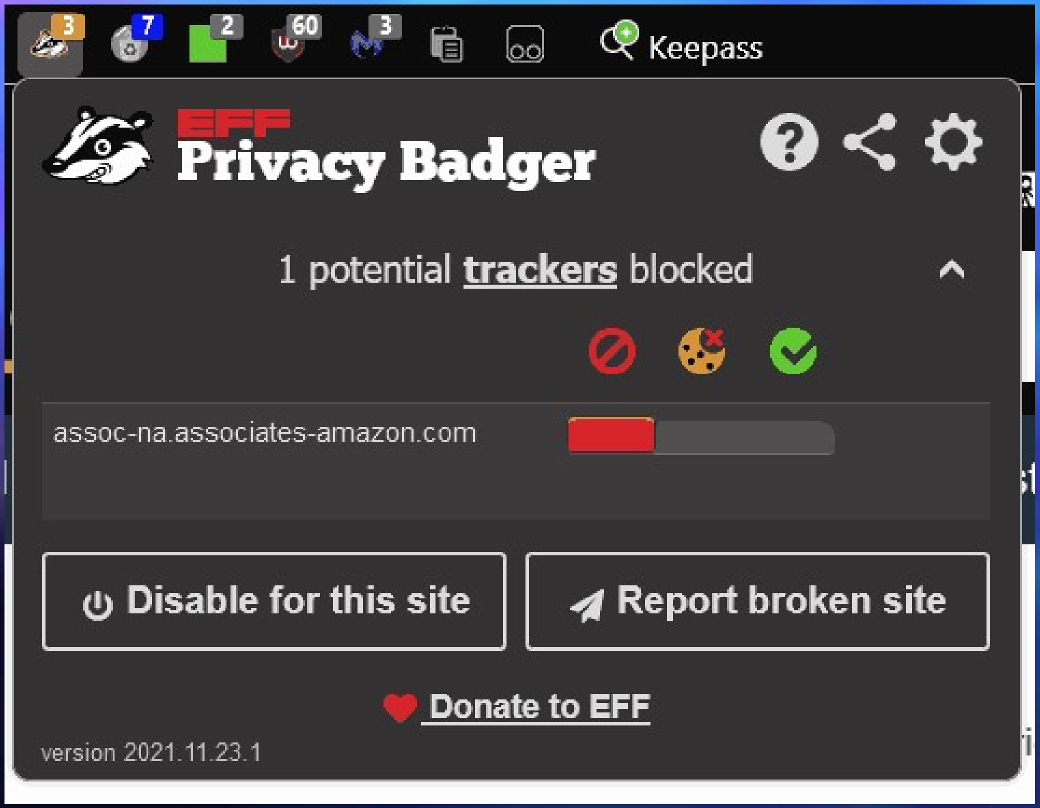
Blocked on this page
1 (3%)

Domains connected
4 out of 5

Blocked since install
1.259M (10%)

Version 1.38.6

Privacy badger



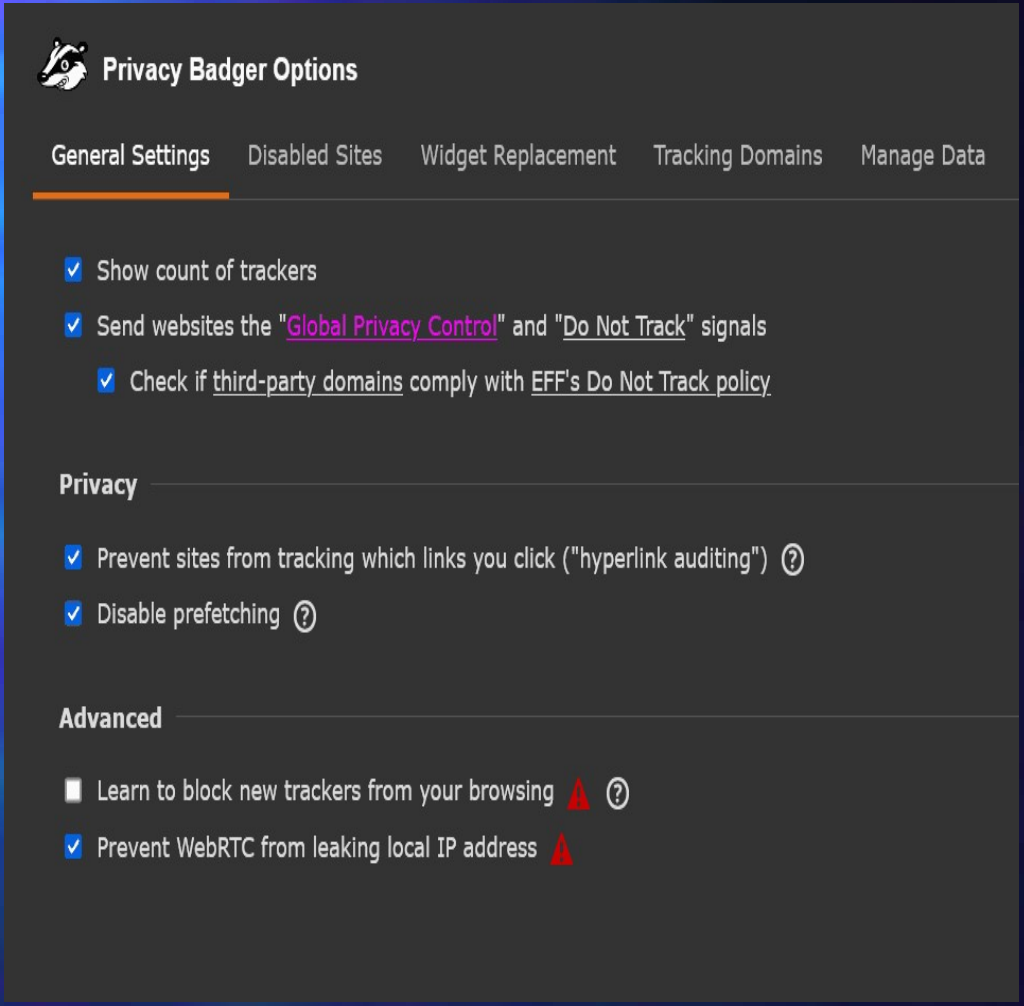
EFF Privacy Badger

1 potential trackers blocked

assoc-na.associates-amazon.com	🟥

Donate to EFF

version 2021.11.23.1


Privacy Badger Options

- ☑ Show count of trackers
- ☑ Send websites the "Global Privacy Control" and "Do Not Track" signals
  - ☑ Check if third-party domains comply with EFF's Do Not Track policy

Privacy

- ☑ Prevent sites from tracking which links you click ("hyperlink auditing") ?
- ☑ Disable prefetching ?

Advanced

- □ Learn to block new trackers from your browsing ⚠ ?
- ☑ Prevent WebRTC from leaking local IP address ⚠

Detection

- https://haveibeenpwned.com/
- Virus scans
  - Windows
- Phishing/popup awareness
  - Don’t click links!
- POPfile
- Winpatrol
- WifiGuard

Virus scans

- Bootable Offline virus scans available
  - Safer
  - Works with dead systems
  - https://www.raymond.cc/blog/portable-emsisoft-anti-malware-5-0-from-free-emergency-kit/

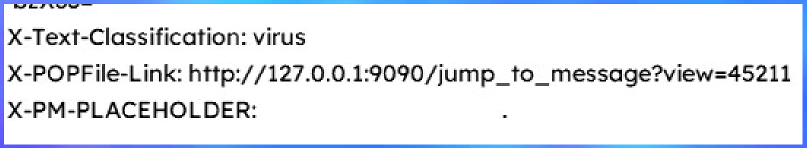
Phishing/popup awareness

- Phishing emails/posts/popups often look like:
  - Friends’ links!
  - Deliveries
  - Invoices
  - Email host hiccups
  - Bank notices
- Don’t click! Use your or google links to correct site.

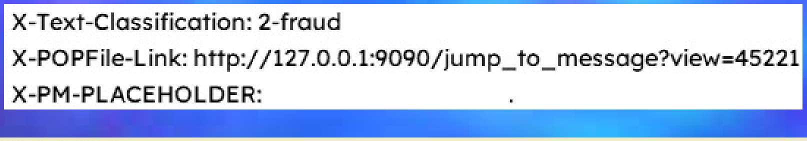
POPfile

- Used with offline mail like Outlook, Thunderbird
- Acts as proxy to get mail
- Uses bayseian logic to classify email

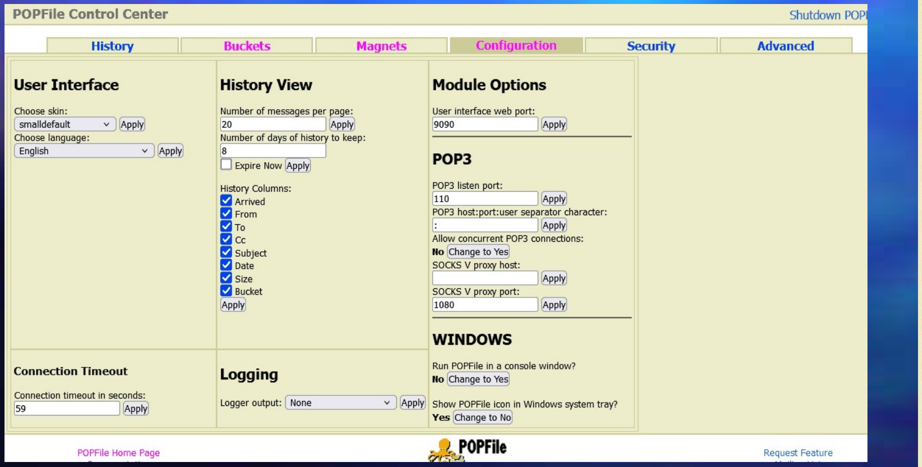
Popfile



X-Text-Classification: virus
X-POPFile-Link: http://127.0.0.1:9090/jump_to_message?view=45211
X-PM-PLACEHOLDER: .



X-Text-Classification: 2-fraud
X-POPFile-Link: http://127.0.0.1:9090/jump_to_message?view=45221
X-PM-PLACEHOLDER: .



POPFile Control Center

User Interface

Choose skin: smalldefault Apply
Choose language: English Apply

History View

Number of messages per page: 20 Apply
Number of days of history to keep: 8
□ Expire Now Apply

History Columns:
☑ Arrived
☑ From
☑ To
☑ Cc
☑ Subject
☑ Date
☑ Size
☑ Bucket
Apply

Module Options

User interface web port: 9090 Apply

POP3

POP3 listen port: 110 Apply
POP3 host:port:user separator character: : Apply
Allow concurrent POP3 connections:
No Change to Yes
SOCKS V proxy host: Apply
SOCKS V proxy port: 1080 Apply

WINDOWS

Run POPFile in a console window?
No Change to Yes

Show POPFile icon in Windows system tray?
Yes Change to No

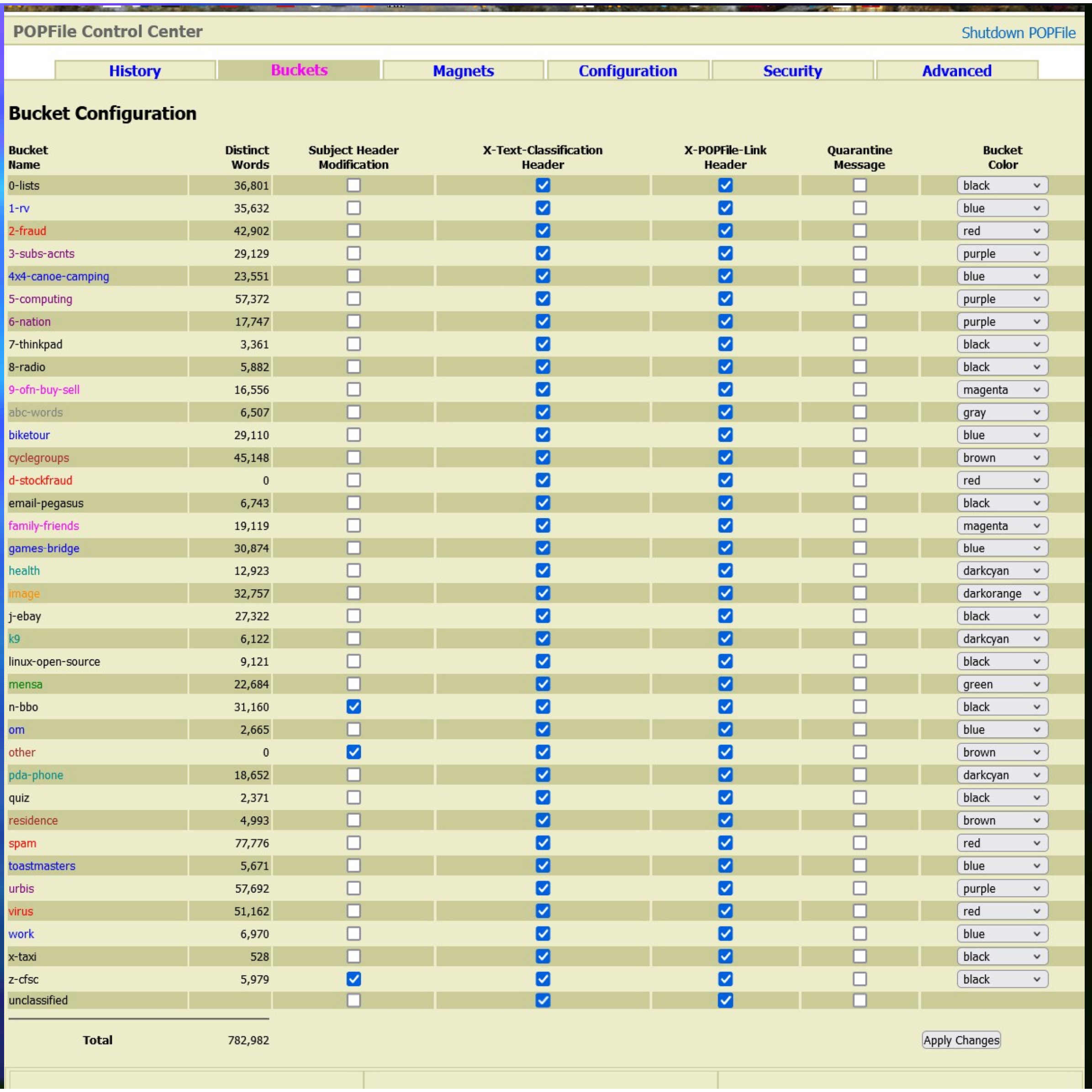
Connection Timeout

Connection timeout in seconds: 59 Apply

Logging

Logger output: None Apply

2021 Dec 8



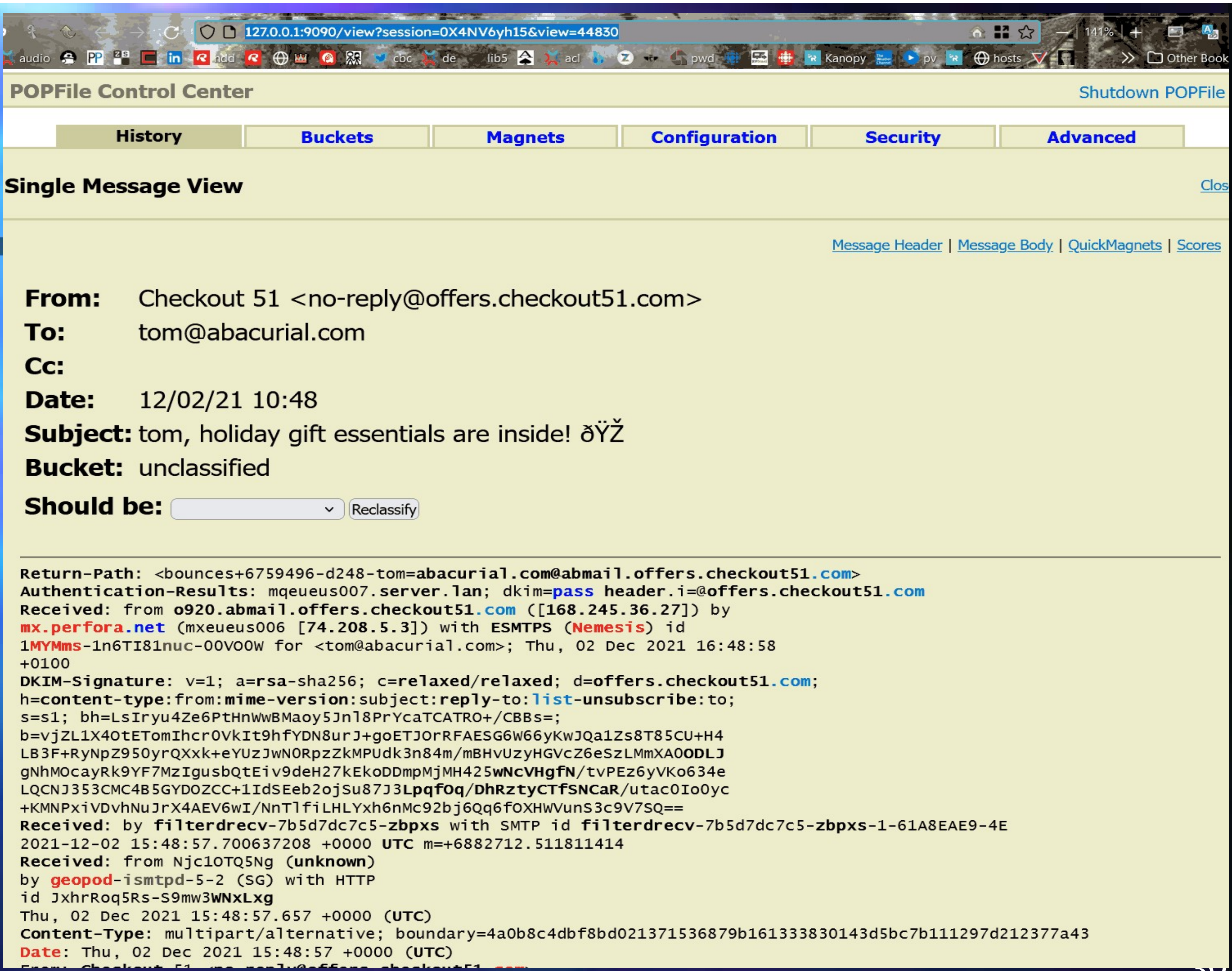
POPFile Control Center

Bucket Configuration

Bucket Name	Distinct Words	Subject Header Modification	X-Text-Classification Header	X-POPFile-Link Header	Quarantine Message	Bucket Color
0-lists	36,801	□	☑	☑	□	black
1-rv	35,632	□	☑	☑	□	blue
2-fraud	42,902	□	☑	☑	□	red
3-subs-acnts	29,129	□	☑	☑	□	purple
4x4-canoe-camping	23,551	□	☑	☑	□	blue
5-computing	57,372	□	☑	☑	□	purple
6-nation	17,747	□	☑	☑	□	purple
7-thinkpad	3,361	□	☑	☑	□	black
8-radio	5,882	□	☑	☑	□	black
9-ofn-buy-sell	16,556	□	☑	☑	□	magenta
abc-words	6,507	□	☑	☑	□	gray
biketour	29,110	□	☑	☑	□	blue
cyclegroups	45,148	□	☑	☑	□	brown
d-stockfraud	0	□	☑	☑	□	red
email-pegasus	6,743	□	☑	☑	□	black
family-friends	19,119	□	☑	☑	□	magenta
games-bridge	30,874	□	☑	☑	□	blue
health	12,923	□	☑	☑	□	darkcyan
image	32,757	□	☑	☑	□	darkorange
j-ebay	27,322	□	☑	☑	□	black
k9	6,122	□	☑	☑	□	darkcyan
linux-open-source	9,121	□	☑	☑	□	black
mensa	22,684	□	☑	☑	□	green
n-bbo	31,160	☑	☑	☑	□	black
om	2,665	□	☑	☑	□	blue
other	0	☑	☑	☑	□	brown
pda-phone	18,652	□	☑	☑	□	darkcyan
quiz	2,371	□	☑	☑	□	black
residence	4,993	□	☑	☑	□	brown
spam	77,776	□	☑	☑	□	red
toastmasters	5,671	□	☑	☑	□	blue
urbis	57,692	□	☑	☑	□	purple
virus	51,162	□	☑	☑	□	red
work	6,970	□	☑	☑	□	blue
x-taxi	528	□	☑	☑	□	black
z-cfsc	5,979	☑	☑	☑	□	black
unclassified		□	☑	☑	□	
Total	782,982					Apply Changes

Popfile

- Teaching Popfile

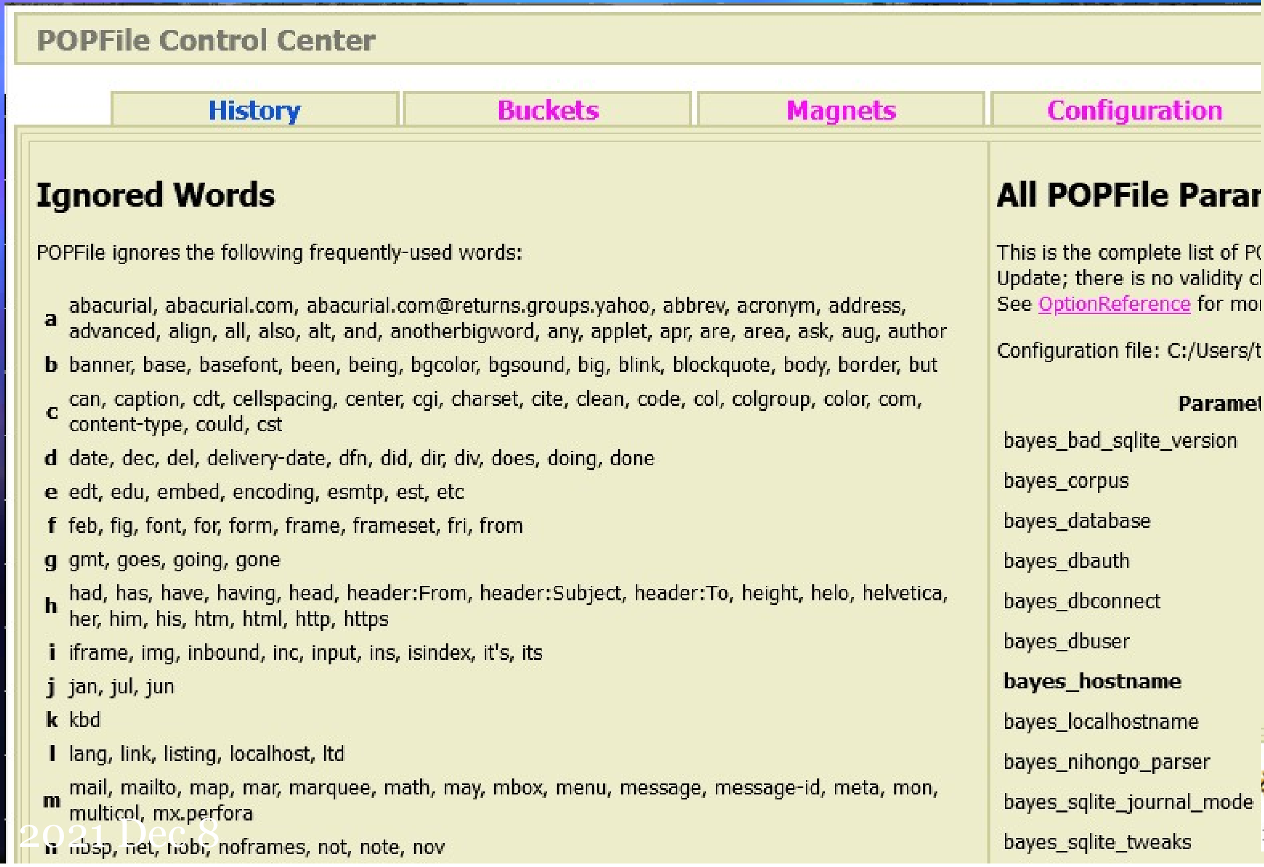


Single Message View

From: Checkout 51 <no-reply@offers.checkout51.com>
To: tom@abacurial.com
Cc:
Date: 12/02/21 10:48
Subject: tom, holiday gift essentials are inside! ðŸŽ
Bucket: unclassified
Should be:

```
Return-Path: <bounces+6759496-d248-tom=abacurial.com@abmail.offers.checkout51.com>
Authentication-Results: mqeueus007.server.lan; dkim=pass header.i=@offers.checkout51.com
Received: from o920.abmail.offers.checkout51.com ([168.245.36.27]) by
mx.perfora.net (mxeueus006 [74.208.5.3]) with ESMTPS (Nemesis) id
1MYMms-1n6TI81nuc-00VO0W for <tom@abacurial.com>; Thu, 02 Dec 2021 16:48:58
+0100
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=offers.checkout51.com;
h=content-type:from:mime-version:subject:reply-to:list-unsubscribe:to;
s=s1; bh=LsIryu4Ze6PtHnWwBMaoy5Jnl8PrYcaTCATRO+/CBBs=;
b=vjZL1X4OtETomIhcr0VkIt9hfYDN8urJ+goETJOrRFAESG6W66yKwJQa1Zs8T85CU+H4
LB3F+RyNpZ95OyrQXxk+eYUzJwNORpzZkMPUdk3n84m/mBHvUzyHGVcZ6eSzLMmXA0ODLJ
gNhMOcayRk9YF7MzIgusbQtEiv9deH27kEkoDDmpMjMH425wNcVHgfN/tvPEz6yVKo634e
LQCNJ353CMC4B5GYDOZCC+1IdSEeb2ojSu87J3LpqfOq/DhRztyCTfSNCaR/utac0Io0yc
+KMNPxiVDvhNuJrX4AEV6wI/NnTlfiLHLYxh6nMc92bj6Qq6fOXHWVunS3c9V7SQ==
Received: by filterdrecv-7b5d7dc7c5-zbpxs with SMTP id filterdrecv-7b5d7dc7c5-zbpxs-1-61A8EAE9-4E
2021-12-02 15:48:57.700637208 +0000 UTC m=+6882712.511811414
Received: from Njc1OTQ5Ng (unknown)
by geopod-ismtpd-5-2 (SG) with HTTP
id JxhrRoq5Rs-S9mw3WNxLxg
Thu, 02 Dec 2021 15:48:57.657 +0000 (UTC)
Content-Type: multipart/alternative; boundary=4a0b8c4dbf8bd021371536879b161333830143d5bc7b111297d212377a43
Date: Thu, 02 Dec 2021 15:48:57 +0000 (UTC)
From: Checkout 51 <no-reply@offers.checkout51.com>
```

Popfile



POPFile Control Center

Ignored Words

POPFile ignores the following frequently-used words:

a abacurial, abacurial.com, abacurial.com@returns.groups.yahoo, abbrev, acronym, address, advanced, align, all, also, alt, and, anotherbigword, any, applet, apr, are, area, ask, aug, author

b banner, base, basefont, been, being, bgcolor, bgsound, big, blink, blockquote, body, border, but

c can, caption, cdt, cellspacing, center, cgi, charset, cite, clean, code, col, colgroup, color, com, content-type, could, cst

d date, dec, del, delivery-date, dfn, did, dir, div, does, doing, done

e edt, edu, embed, encoding, esmtp, est, etc

f feb, fig, font, for, form, frame, frameset, fri, from

g gmt, goes, going, gone

h had, has, have, having, head, header:From, header:Subject, header:To, height, helo, helvetica, her, him, his, htm, html, http, https

i iframe, img, inbound, inc, input, ins, isindex, it's, its

j jan, jul, jun

k kbd

l lang, link, listing, localhost, ltd

m mail, mailto, map, mar, marquee, math, may, mbox, menu, message, message-id, meta, mon, multicol, mx.perfora

n nbsp, net, nobr, noframes, not, note, nov

All POPFile Parar

This is the complete list of P(
Update; there is no validity cl
See OptionReference for mor

Configuration file: C:/Users/t

Paramet

bayes_bad_sqlite_version

bayes_corpus

bayes_database

bayes_dbauth

bayes_dbconnect

bayes_dbuser

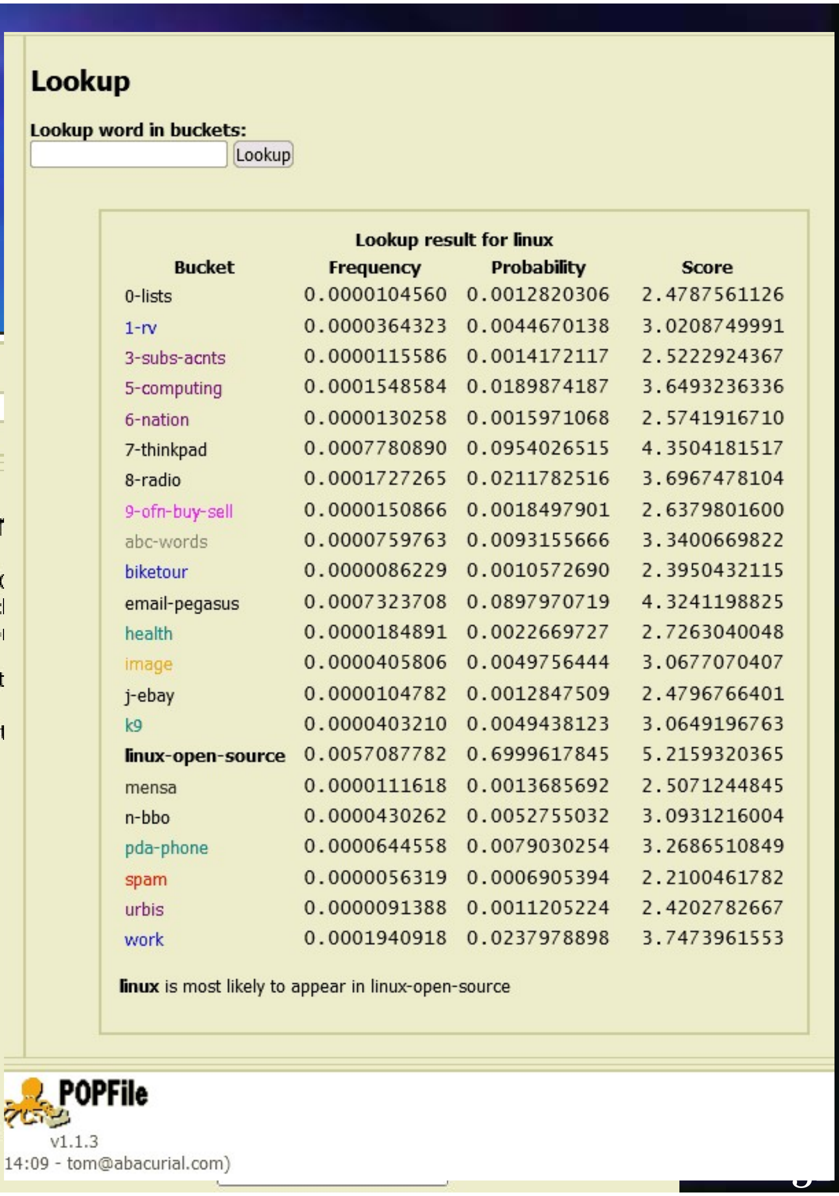
bayes_hostname

bayes_localhostname

bayes_nihongo_parser

bayes_sqlite_journal_mode

bayes_sqlite_tweaks



Lookup

Lookup word in buckets:

Lookup result for linux

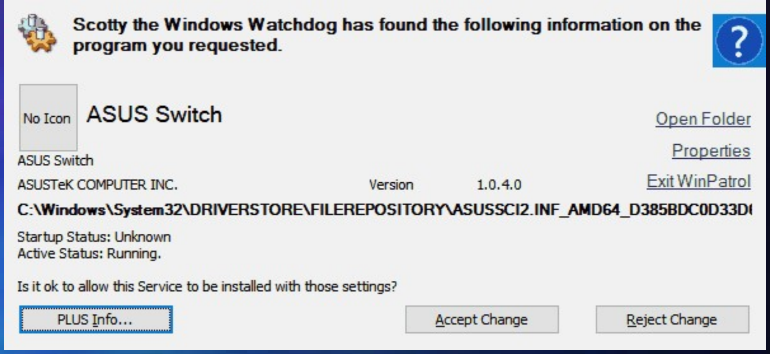
Bucket	Frequency	Probability	Score
0-lists	0.0000104560	0.0012820306	2.4787561126
1-rv	0.0000364323	0.0044670138	3.0208749991
3-subs-acnts	0.0000115586	0.0014172117	2.5222924367
5-computing	0.0001548584	0.0189874187	3.6493236336
6-nation	0.0000130258	0.0015971068	2.5741916710
7-thinkpad	0.0007780890	0.0954026515	4.3504181517
8-radio	0.0001727265	0.0211782516	3.6967478104
9-ofn-buy-sell	0.0000150866	0.0018497901	2.6379801600
abc-words	0.0000759763	0.0093155666	3.3400669822
biketour	0.0000086229	0.0010572690	2.3950432115
email-pegasus	0.0007323708	0.0897970719	4.3241198825
health	0.0000184891	0.0022669727	2.7263040048
image	0.0000405806	0.0049756444	3.0677070407
j-ebay	0.0000104782	0.0012847509	2.4796766401
k9	0.0000403210	0.0049438123	3.0649196763
linux-open-source	0.0057087782	0.6999617845	5.2159320365
mensa	0.0000111618	0.0013685692	2.5071244845
n-bbo	0.0000430262	0.0052755032	3.0931216004
pda-phone	0.0000644558	0.0079030254	3.2686510849
spam	0.0000056319	0.0006905394	2.2100461782
urbis	0.0000091388	0.0011205224	2.4202782667
work	0.0001940918	0.0237978898	3.7473961553

linux is most likely to appear in linux-open-source

POPFile
v1.1.3
14:09 - tom@abacurial.com)

Winpatrol

- Abandonware
- Alerts changes to startup programs



Scotty the Windows Watchdog has found the following information on the program you requested.

No Icon ASUS Switch

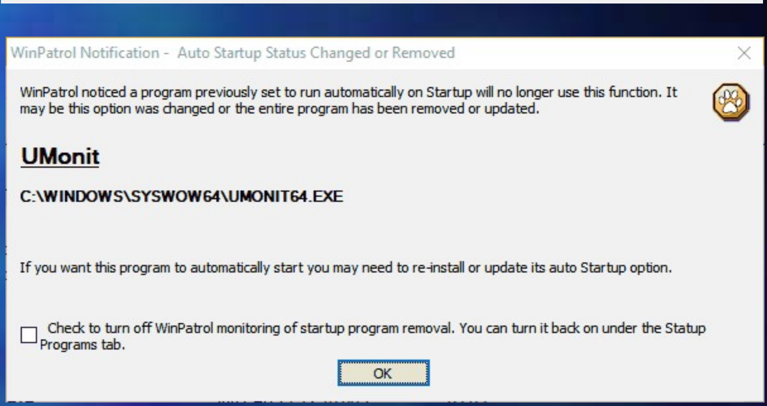
ASUS Switch

ASUSTeK COMPUTER INC. Version 1.0.4.0

C:\Windows\System32\DRIVERSTORE\FILEREPOSITORY\ASUSSCI2.INF_AMD64_D385BDC0D33D

Startup Status: Unknown
Active Status: Running.

Is it ok to allow this Service to be installed with those settings?



WinPatrol Notification - Auto Startup Status Changed or Removed

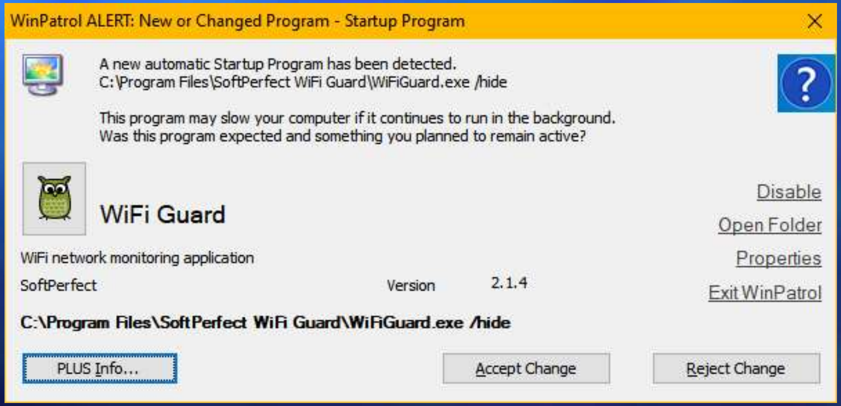
WinPatrol noticed a program previously set to run automatically on Startup will no longer use this function. It may be this option was changed or the entire program has been removed or updated.

UMonit

C:\WINDOWS\SYSWOW64\UMONIT64.EXE

If you want this program to automatically start you may need to re-install or update its auto Startup option.

□ Check to turn off WinPatrol monitoring of startup program removal. You can turn it back on under the Statup Programs tab.



WinPatrol ALERT: New or Changed Program - Startup Program

A new automatic Startup Program has been detected.
C:\Program Files\SoftPerfect WiFi Guard\WiFiGuard.exe /hide

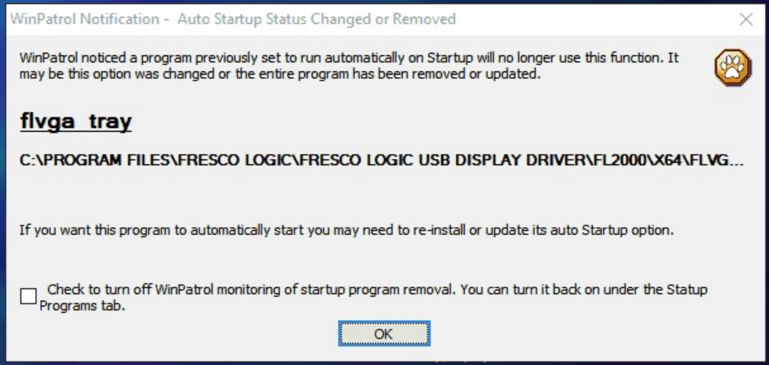
This program may slow your computer if it continues to run in the background.
Was this program expected and something you planned to remain active?

WiFi Guard

WiFi network monitoring application

SoftPerfect Version 2.1.4

C:\Program Files\SoftPerfect WiFi Guard\WiFiGuard.exe /hide



WinPatrol Notification - Auto Startup Status Changed or Removed

WinPatrol noticed a program previously set to run automatically on Startup will no longer use this function. It may be this option was changed or the entire program has been removed or updated.

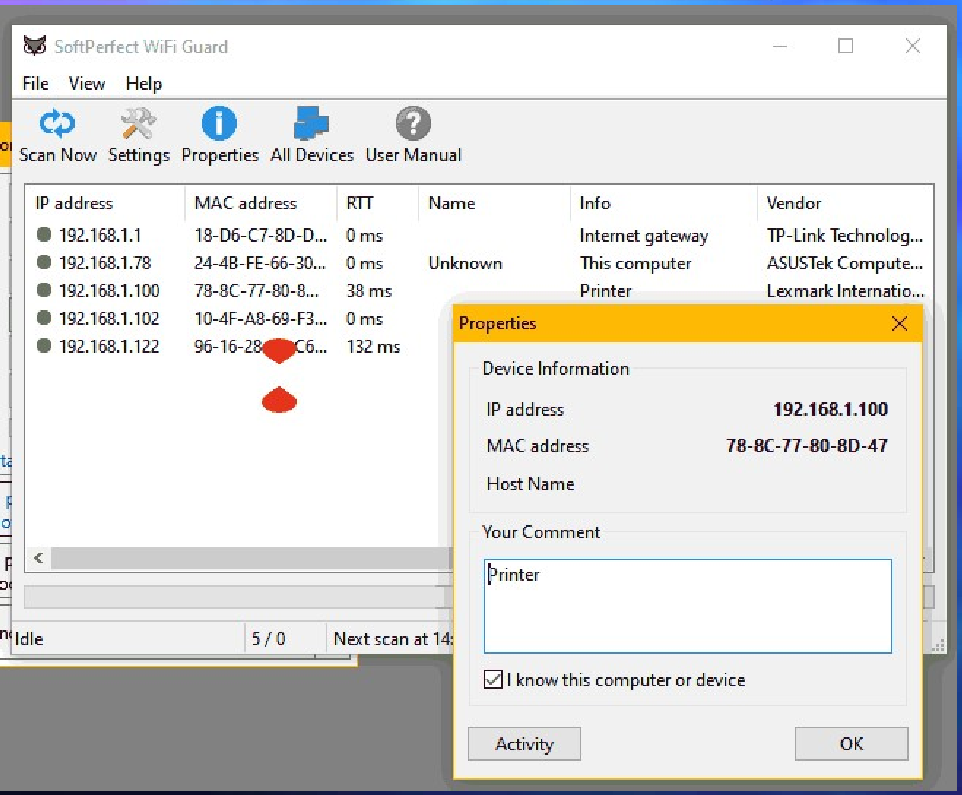
flvga_tray

C:\PROGRAM FILES\FRESCO LOGIC\FRESCO LOGIC USB DISPLAY DRIVER\FL2000\X64\FLVG...

If you want this program to automatically start you may need to re-install or update its auto Startup option.

□ Check to turn off WinPatrol monitoring of startup program removal. You can turn it back on under the Statup Programs tab.

WifiGuard



IP address	MAC address	RTT	Name	Info	Vendor
● 192.168.1.1	18-D6-C7-8D-D...	0 ms		Internet gateway	TP-Link Technolog...
● 192.168.1.78	24-4B-FE-66-30...	0 ms	Unknown	This computer	ASUSTek Compute...
● 192.168.1.100	78-8C-77-80-8...	38 ms		Printer	Lexmark Internatio...
● 192.168.1.102	10-4F-A8-69-F3...	0 ms			
● 192.168.1.122	96-16-28[redacted]C6...	132 ms			

Idle | 5 / 0 | Next scan at 14:

Properties

Device Information

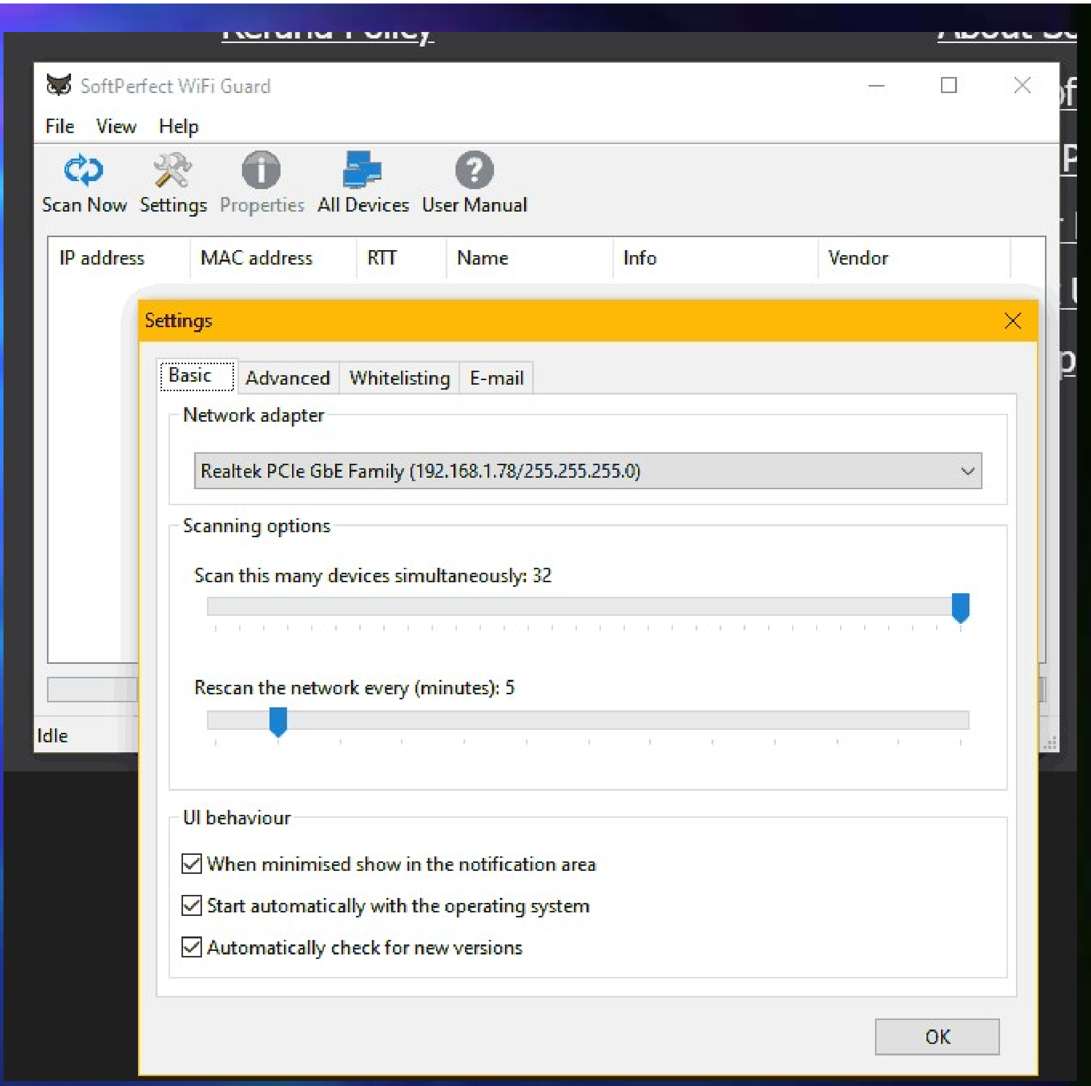
IP address: 192.168.1.100

MAC address: 78-8C-77-80-8D-47

Host Name

Your Comment: Printer

☑ I know this computer or device



Settings

Basic | Advanced | Whitelisting | E-mail

Network adapter

Realtek PCIe GbE Family (192.168.1.78/255.255.255.0)

Scanning options

Scan this many devices simultaneously: 32

Rescan the network every (minutes): 5

UI behaviour

☑ When minimised show in the notification area

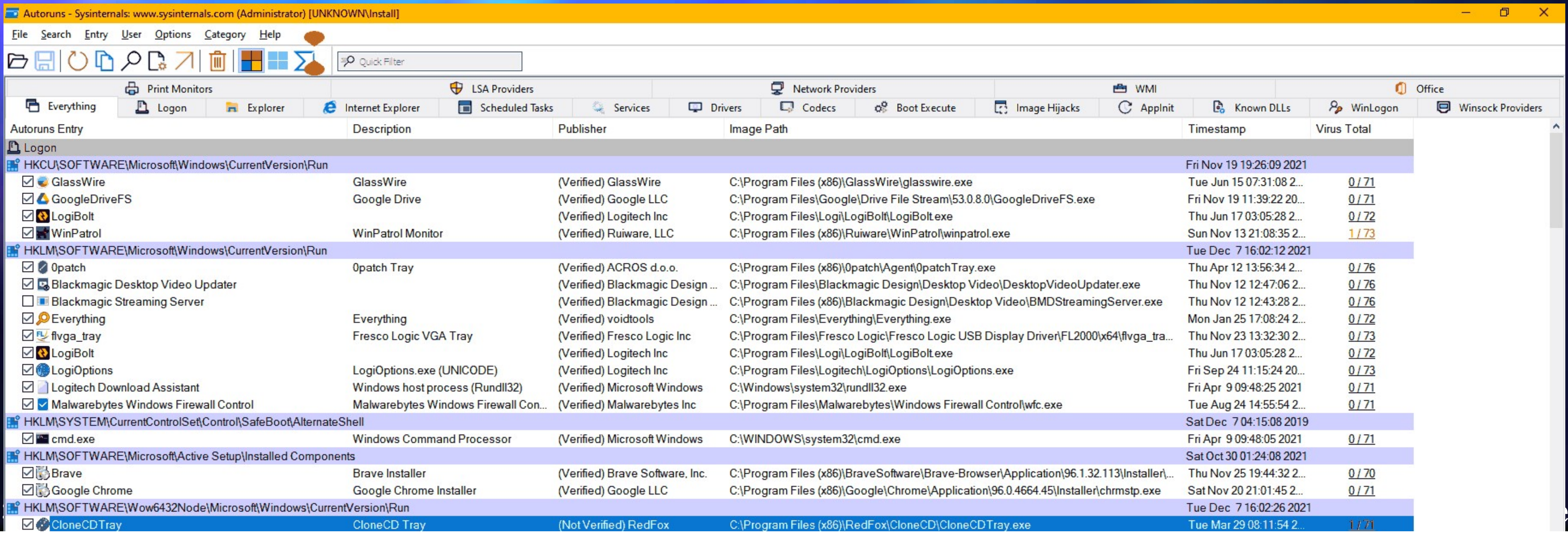
☑ Start automatically with the operating system

☑ Automatically check for new versions

2021 Dec 8

Autoruns

- Microsoft program
- https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns



Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Logon					
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Fri Nov 19 19:26:09 2021	
☑ GlassWire	GlassWire	(Verified) GlassWire	C:\Program Files (x86)\GlassWire\glasswire.exe	Tue Jun 15 07:31:08 2...	0 / 71
☑ GoogleDriveFS	Google Drive	(Verified) Google LLC	C:\Program Files\Google\Drive File Stream\53.0.8.0\GoogleDriveFS.exe	Fri Nov 19 11:39:22 20...	0 / 71
☑ LogiBolt		(Verified) Logitech Inc	C:\Program Files\Logi\LogiBolt\LogiBolt.exe	Thu Jun 17 03:05:28 2...	0 / 72
☑ WinPatrol	WinPatrol Monitor	(Verified) Ruiware, LLC	C:\Program Files (x86)\Ruiware\WinPatrol\winpatrol.exe	Sun Nov 13 21:08:35 2...	1 / 73
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Tue Dec 7 16:02:12 2021	
☑ 0patch	0patch Tray	(Verified) ACROS d.o.o.	C:\Program Files (x86)\0patch\Agent\0patchTray.exe	Thu Apr 12 13:56:34 2...	0 / 76
☑ Blackmagic Desktop Video Updater		(Verified) Blackmagic Design ...	C:\Program Files\Blackmagic Design\Desktop Video\DesktopVideoUpdater.exe	Thu Nov 12 12:47:06 2...	0 / 76
☐ Blackmagic Streaming Server		(Verified) Blackmagic Design ...	C:\Program Files (x86)\Blackmagic Design\Desktop Video\BMDStreamingServer.exe	Thu Nov 12 12:43:28 2...	0 / 76
☑ Everything	Everything	(Verified) voidtools	C:\Program Files\Everything\Everything.exe	Mon Jan 25 17:08:24 2...	0 / 72
☑ flvga_tray	Fresco Logic VGA Tray	(Verified) Fresco Logic Inc	C:\Program Files\Fresco Logic\Fresco Logic USB Display Driver\FL2000\x64\flvga_tra...	Thu Nov 23 13:32:30 2...	0 / 73
☑ LogiBolt		(Verified) Logitech Inc	C:\Program Files\Logi\LogiBolt\LogiBolt.exe	Thu Jun 17 03:05:28 2...	0 / 72
☑ LogiOptions	LogiOptions.exe (UNICODE)	(Verified) Logitech Inc	C:\Program Files\Logitech\LogiOptions\LogiOptions.exe	Fri Sep 24 11:15:24 20...	0 / 73
☑ Logitech Download Assistant	Windows host process (Rundll32)	(Verified) Microsoft Windows	C:\Windows\system32\rundll32.exe	Fri Apr 9 09:48:25 2021	0 / 71
☑ Malwarebytes Windows Firewall Control	Malwarebytes Windows Firewall Con...	(Verified) Malwarebytes Inc	C:\Program Files\Malwarebytes\Windows Firewall Control\wfc.exe	Tue Aug 24 14:55:54 2...	0 / 71
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Sat Dec 7 04:15:08 2019	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\WINDOWS\system32\cmd.exe	Fri Apr 9 09:48:05 2021	0 / 71
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Sat Oct 30 01:24:08 2021	
☑ Brave	Brave Installer	(Verified) Brave Software, Inc.	C:\Program Files (x86)\BraveSoftware\Brave-Browser\Application\96.1.32.113\Installer\...	Thu Nov 25 19:44:32 2...	0 / 70
☑ Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files (x86)\Google\Chrome\Application\96.0.4664.45\Installer\chrmstp.exe	Sat Nov 20 21:01:45 2...	0 / 71
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				Tue Dec 7 16:02:26 2021	
☑ CloneCDTray	CloneCD Tray	(Not Verified) RedFox	C:\Program Files (x86)\RedFox\CloneCD\CloneCDTray.exe	Tue Mar 29 08:11:54 2...	1 / 71

Security layers

- No single magic bullet
- Action + awareness
- Good Luck!