Sun City Computer Club

Cyber Security SIG

April 16, 2020

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

- Zoom info, garage door, stimulus scams, etc.

Zoom info

SCCCCyber

Tuesday, March 31, 2020

zoom

The computer club mentioned zoom as an app to do free video conferencing during the stay-at-home period.

Zoom Technologies (ZOOM) stock trading was halted after soaring 56,000%. Wrong zoom.

Zoom, the app for video conferencing has experienced a large increase of use recently.

Helpful <-> Harmful

The installer for zoom on MacOS installs without having a user approve.

Blog Archive

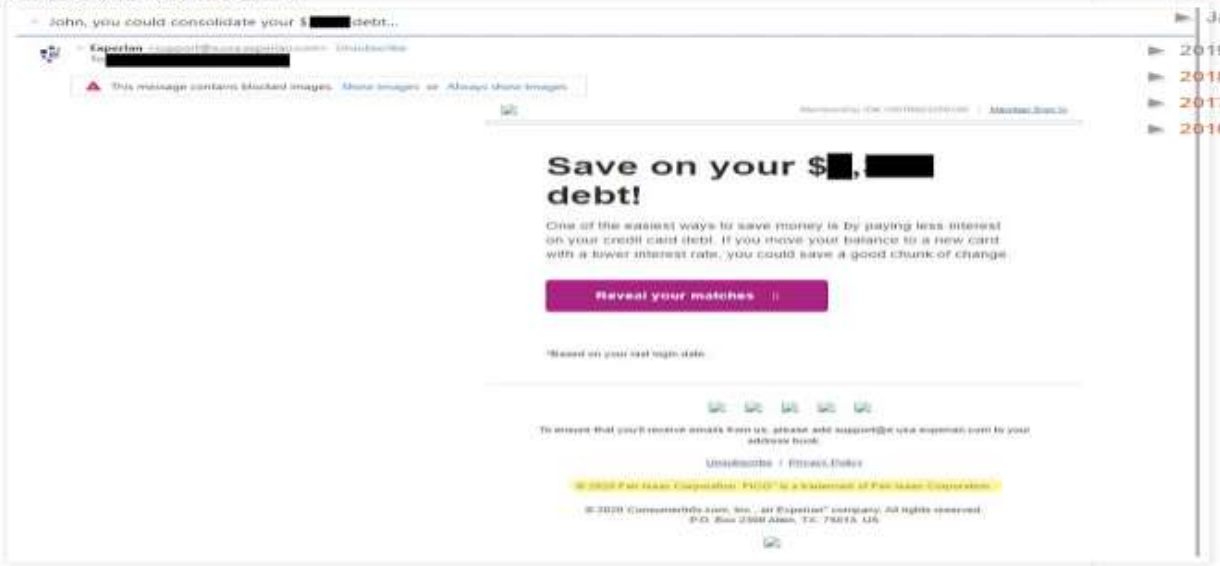
▼ 2020 (16)
▼ April (1)
Home Garage and Automobile security
▼ March (8)
zoom
patches and updates abound 24-Mar-2020
Yet another Microsoft Windows zero-day vulnerabili...
COVID-19 related scams, links, false information, ...
COVID-19 and privacy/tracking?
Rumors of US national quarantine are FAKE
Got iPhone? Got unexplained cellular data?
Out of Band Microsoft security Update KB4551762
► February (3)
► January (4)
► 2019 (28)
► 2018 (57)
► 2017 (62)
► 2016 (16)

Wednesday, April 8, 2020

Experian crossing creepy line?

Google's CEO said "Google policy on a lot of these things is to get right up to the creepy line and not cross it."
I feel the creepy line in my opinion has been crossed at times.

Then today we got this eMail:



So the subject line has an explicit amount and a name on the subject line. Bad practice. The amount cited is an exact figure of a recent change yesterday. Our bank online statement still does NOT list this charge at the time of this post.
The message headers indicate this is sent MIME to get the images and graphics. Not S/MIME.
I didn't know FICO legal name was Fair Isaac Corporation.

Equifax, Experian, TJ Maxx, Ashley Madison, Target, zoom, Marriott, ...
We are all in this together. *They* are also all in this together.

Awareness, Preparedness, Understanding.

Live your life like your life has been captured for use. It probably has.

Blog Archive

- 2020 (18)
  - April (3)
    - Experian crossing creepy line?
    - Updates abound 4/7/2020
    - Home Garage and Automobile security
  - March (8)
  - February (3)
  - January (4)
- 2019 (28)
- 2018 (57)
- 2017 (62)
- 2016 (16)

HI, WE'VE CHANGED YOUR PRIVACY SETTINGS.

38
London Life
THE APP TO SAVE US FROM PANDEMIC PANDEMONIUM
PANDEMICS are nothing to be sniffed at. "A flu pandemic will spread through the world so quickly that we won't be able to make vaccines quickly enough," says mathematician Dr Hannah Fry. The first line of defence, therefore, is tech.
Fry and Dr Javid Abdelmoneim have built the BBC Pandemic app to help plot how a disease would spread (a 90-minute associated documentary, BBC Pandemic, will air in spring 2018 on BBC Four). It is free to download and anonymously tracks your location over 24 hours, recording who you have met, and uses the information for the greater good.
"We don't get a trial run for this, it's a case of when not if," says Fry. "When it does happen we need to be able to make sure we're making the right decisions at the right times: should we close the schools and the airports? How many hospital beds do we need?" The Government National Risk Register estimates that infectious diseases are an even greater risk than terrorism.
So how does the app work? "To be able to create a mathematical simulation you need to know how often we come into contact with each other
Summing up: left, Dr Hannah Fry, who has designed Pandemic, far left
ES TRAVEL
the latest outstanding travel offers with these
come with free excursions
The service allows
GP over video lin
Continued from Page 37
Indeed, the country's medical tech

Pandemic

BBC Pandemic

360 PRODUCTION LIMITED **Medical**

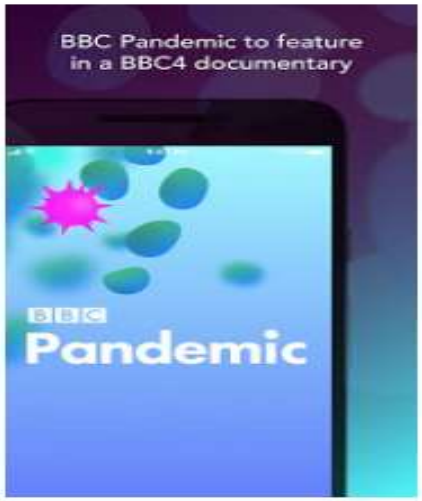
★★☆☆☆ 297

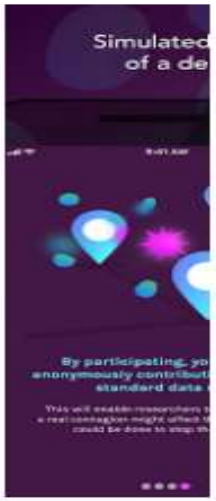
E Everyone

⚠ You don't have any devices.

Add to wishlist

Install





BBC Pandemic gives you the opportunity to be part of a unique experiment that could save lives.

With this app, you can join in a ground-breaking nationwide citizen science experiment that will gather data to help researchers predict the spread of a deadly flu outbreak across the United Kingdom. But don't worry, this will be a life-saving simulated pandemic.

- CPAP machines as ventilators

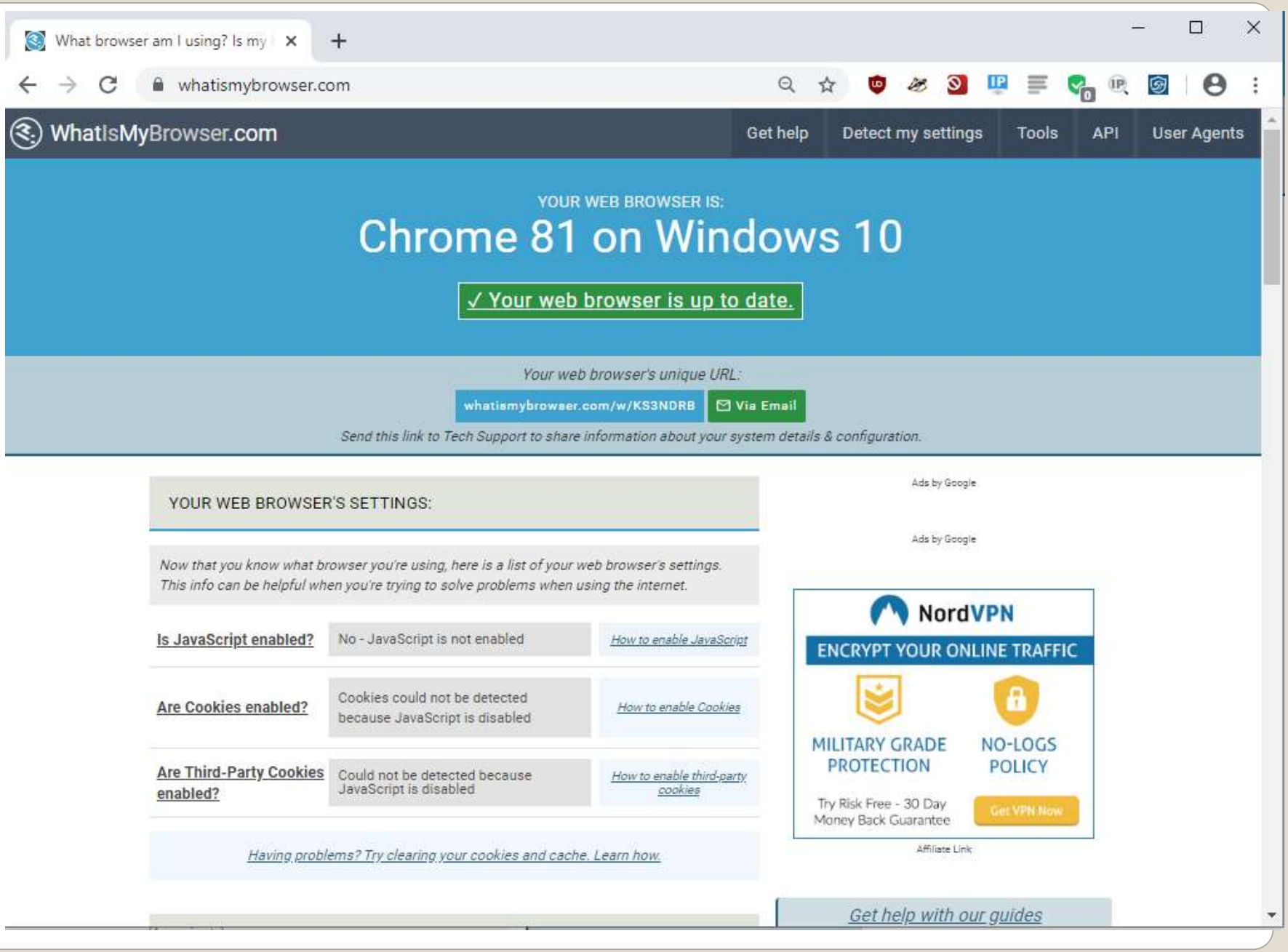
Helpful

- CPAP machines as ventilators
- CPAP machines as ventilators may spread virus

Helpful <-> Harmful

Current Issues

- Stimulusdeposit
- Cobol programmers needed 1999
- Corp.com bought by Microsoft
- Pixel 4 smart phone Android 10
  Facial unlock requires open eyes
- 5G tower sabotage
- iOS iPadOS MacOS Safari update
  Camera and microphone control
- Most browsers have recent updates
- Contractor ransomware data release
- 3D printers high temperature long duty cycle
- Covid-19 Cyber Threat Coalition CTI League
- Whatismybrowser.com


What browser am I using? Is my
whatismybrowser.com
WhatIsMyBrowser.com
Get help
Detect my settings
Tools
API
User Agents
YOUR WEB BROWSER IS:
Chrome 81 on Windows 10
✓ Your web browser is up to date.
Your web browser's unique URL:
whatismybrowser.com/w/KS3NDRB
Via Email
Send this link to Tech Support to share information about your system details & configuration.
YOUR WEB BROWSER'S SETTINGS:
Now that you know what browser you're using, here is a list of your web browser's settings.
This info can be helpful when you're trying to solve problems when using the internet.
Is JavaScript enabled?
No - JavaScript is not enabled
How to enable JavaScript
Are Cookies enabled?
Cookies could not be detected because JavaScript is disabled
How to enable Cookies
Are Third-Party Cookies enabled?
Could not be detected because JavaScript is disabled
How to enable third-party cookies
Having problems? Try clearing your cookies and cache. Learn how.
Ads by Google
Ads by Google
NordVPN
ENCRYPT YOUR ONLINE TRAFFIC
MILITARY GRADE PROTECTION
NO-LOGS POLICY
Try Risk Free - 30 Day Money Back Guarantee
Get VPN Now
Affiliate Link
Get help with our guides

MORE INFO ABOUT YOUR SYSTEM:

EXTRA INFO

Your browser told us a few extra things about your set up...

- **64-bit Edition**

IP ADDRESS

This is your public IP Address.

74.192.[redacted]
Your IP Address can identify you online.
Use a VPN to help stay private and secure.

LOCATION

Your IP address can reveal your location.

Georgetown, United States, Earth
(Approximate)

USING A VPN OR PROXY?

Do you appear to be using a VPN or a proxy on the internet?

Coming soon!
We're building this detection right now and will launch it soon

INCOGNITO MODE / PRIVATE BROWSING

Is your browser recording your history and storing a cache?

Coming soon!
We're building this detection right now and will launch it soon

COMPUTER SCREEN

The dimensions/resolution and color depth of your screen.

Computer screen could not be detected because Javascript is disabled

BROWSER WINDOW SIZE

Including your toolbars.

Browser size could not be detected because Javascript is disabled

"DO NOT TRACK" SETTING

Ask websites to not track you.

"Do Not Track" is Enabled

USING TOR?

Are you using The Onion Router network?

No
It doesn't look like your traffic is coming from a TOR exit node

Confused by this info readout? Here's some help!

How did we find all this information about your browser out?

How can I use this detection on my own site?

Get help with our guides

Getting TLS warnings? Here's why.
Are some websites showing you warnings about out-dated TLS? Here's why it's happening. *Read more*

How to update your browser
Old software puts you at risk. *Read more*

Clear your cookies and history
How to reset your browsing history *Read more*

Try a different web browser
Different web browsers have different features - try a different one to see if you prefer it. *Read more*

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.

Test your server »
Test your site's certificate and configuration

Test your browser »
Test your browser's SSL implementation

SSL Pulse »
See how other web sites are doing

Documentation »
Learn how to deploy SSL/TLS correctly

Books

Bulletproof SSL and TLS is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system administrators, and developers, with the main focus on getting things done. MORE »

News

About SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

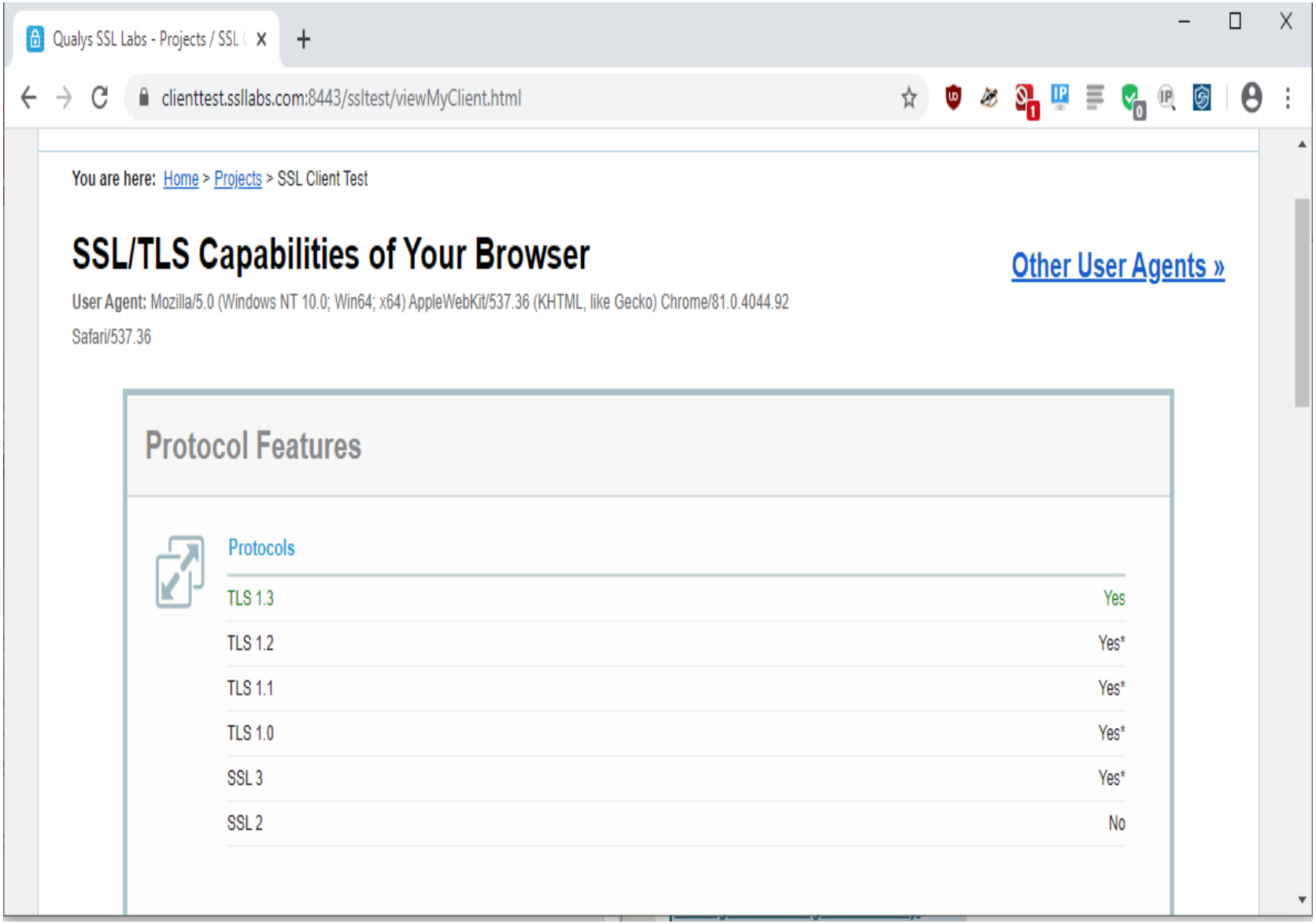
SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- Ivan Ristić, Qualys

Copyright © 2009-2020 Qualys, Inc. All Rights Reserved.

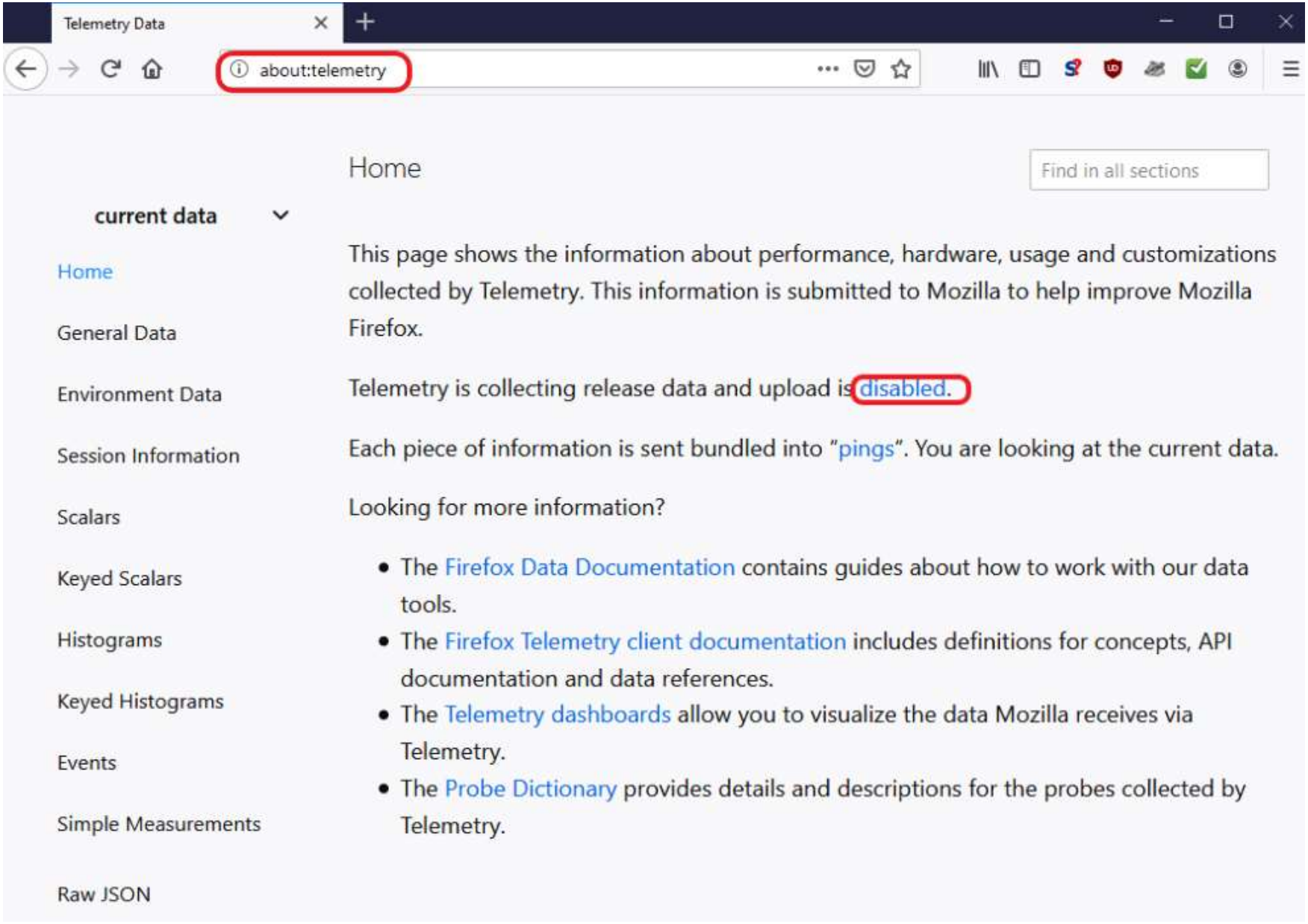
Terms and Conditions

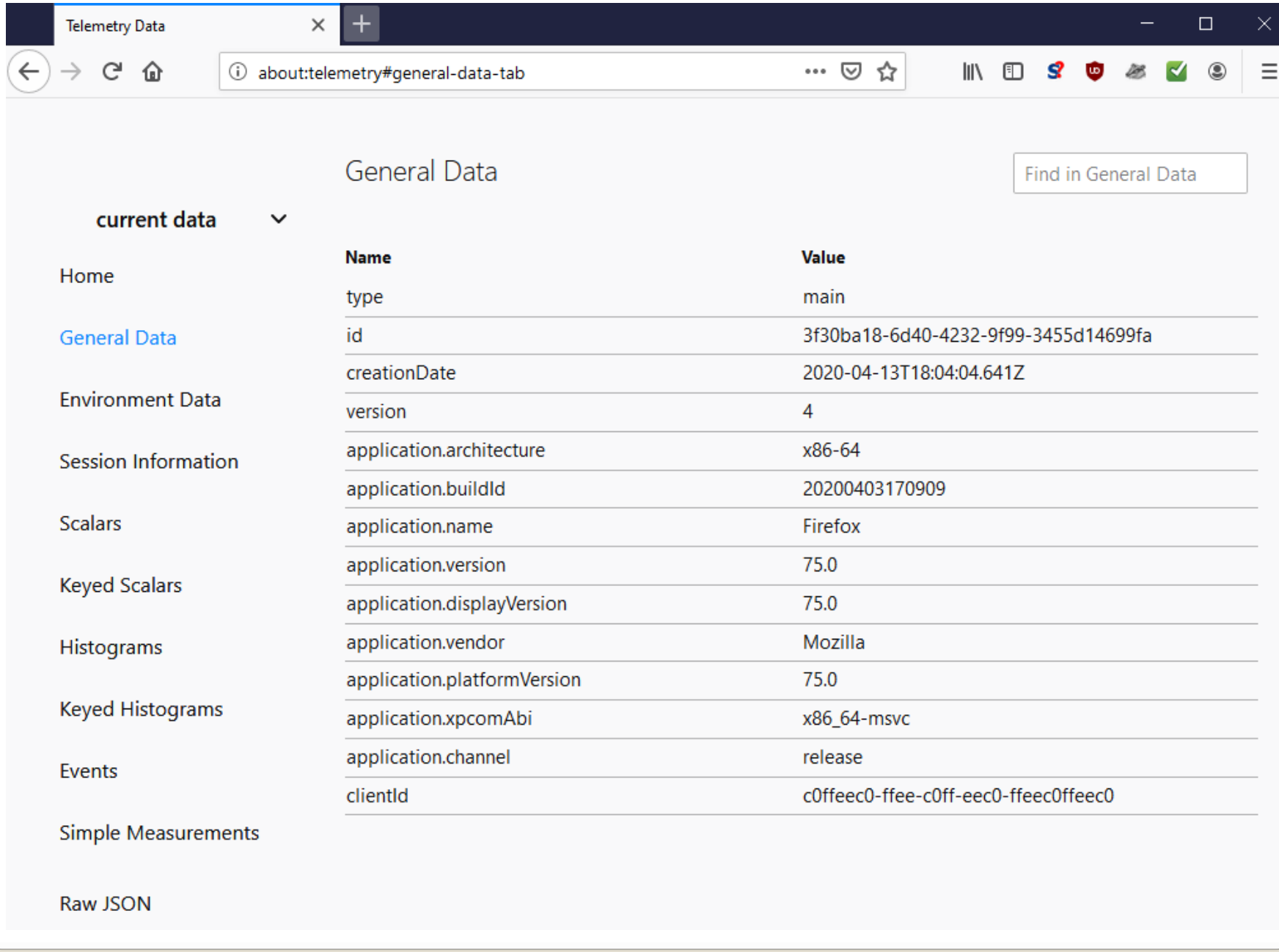
Try Qualys for free! Experience the award-winning Qualys Cloud Platform and the entire collection of Qualys Cloud Apps, including certificate security solutions.

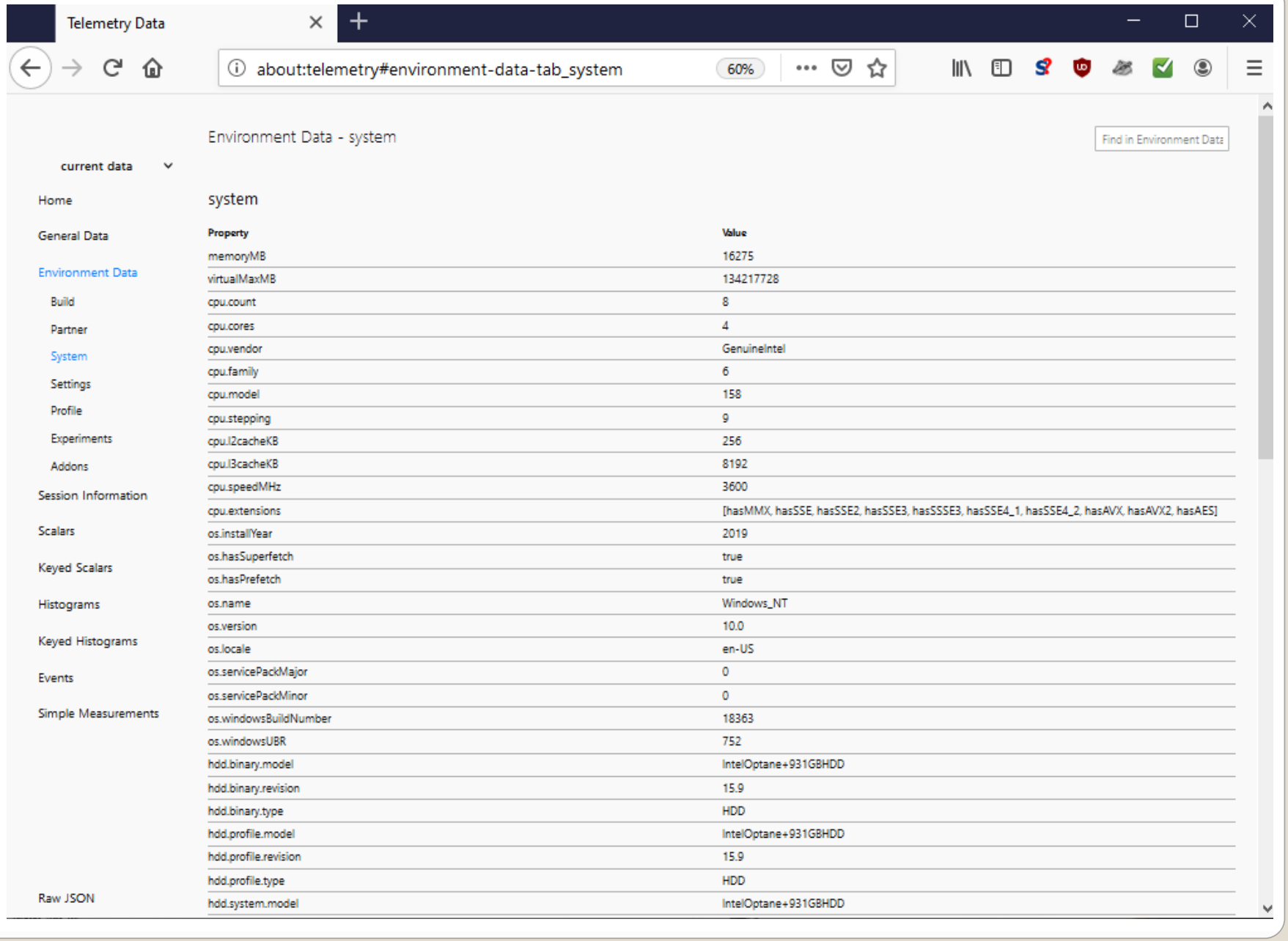

Qualys SSL Labs - Projects / SSL
clienttest.ssllabs.com:8443/ssltest/viewMyClient.html
You are here: Home > Projects > SSL Client Test
SSL/TLS Capabilities of Your Browser
Other User Agents »
User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.92 Safari/537.36
Protocol Features
Protocols
TLS 1.3 Yes
TLS 1.2 Yes*
TLS 1.1 Yes*
TLS 1.0 Yes*
SSL 3 Yes*
SSL 2 No

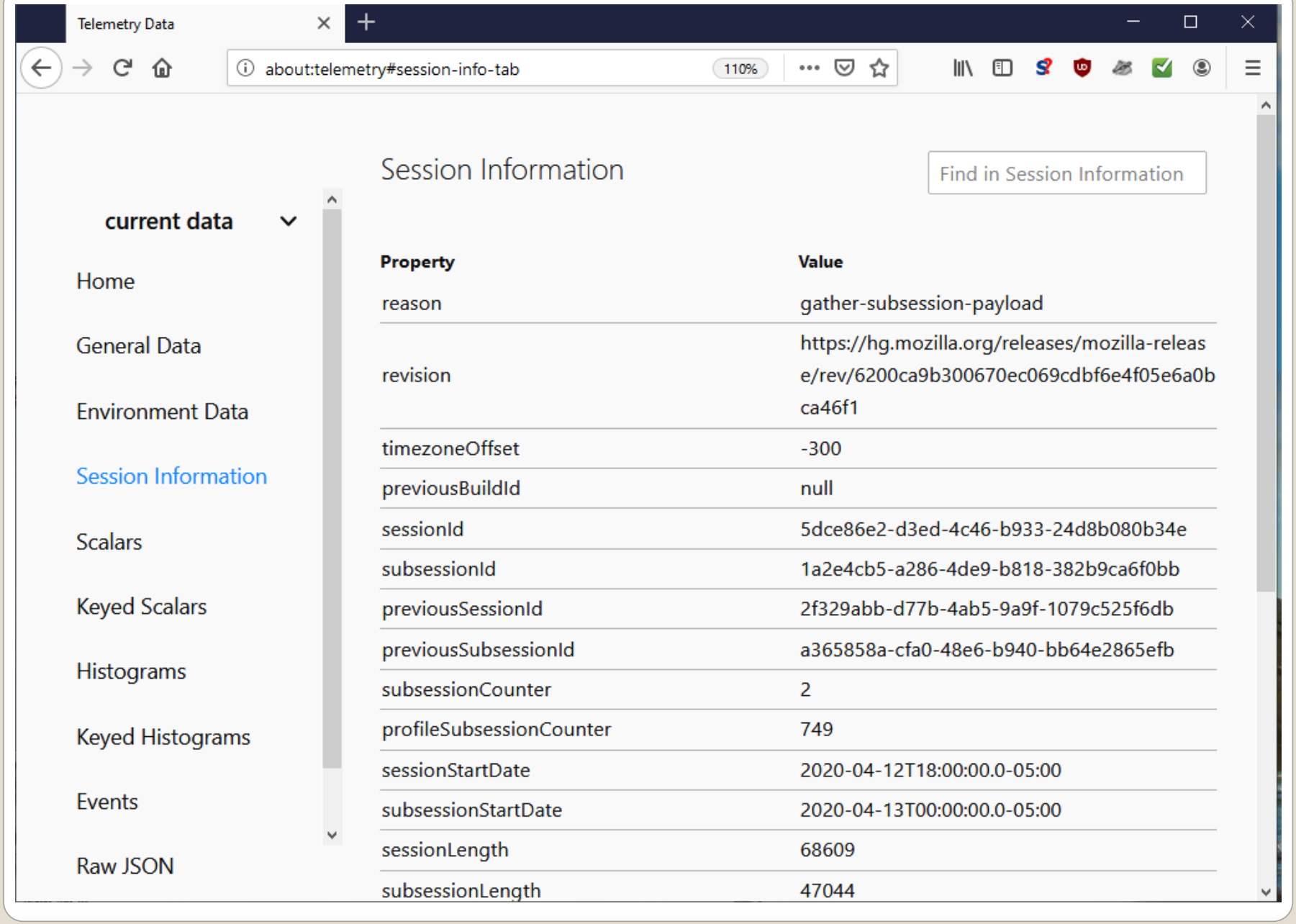
EPSON

- LARGE increase of COVID keywords
- LARGE increase of stolen or cloned eMail
- EVERY browser recent updates
- Firefox 0-day update version 75.
- But then Mozilla scheduled task!


Telemetry Data
about:telemetry
Home
Find in all sections
current data
Home
General Data
Environment Data
Session Information
Scalars
Keyed Scalars
Histograms
Keyed Histograms
Events
Simple Measurements
Raw JSON
This page shows the information about performance, hardware, usage and customizations collected by Telemetry. This information is submitted to Mozilla to help improve Mozilla Firefox.
Telemetry is collecting release data and upload is disabled.
Each piece of information is sent bundled into "pings". You are looking at the current data.
Looking for more information?
The Firefox Data Documentation contains guides about how to work with our data tools.
The Firefox Telemetry client documentation includes definitions for concepts, API documentation and data references.
The Telemetry dashboards allow you to visualize the data Mozilla receives via Telemetry.
The Probe Dictionary provides details and descriptions for the probes collected by Telemetry.


Telemetry Data
about:telemetry#general-data-tab
General Data
Find in General Data
current data
Home
General Data
Environment Data
Session Information
Scalars
Keyed Scalars
Histograms
Keyed Histograms
Events
Simple Measurements
Raw JSON
Name
Value
type
main
id
3f30ba18-6d40-4232-9f99-3455d14699fa
creationDate
2020-04-13T18:04:04.641Z
version
4
application.architecture
x86-64
application.buildId
20200403170909
application.name
Firefox
application.version
75.0
application.displayVersion
75.0
application.vendor
Mozilla
application.platformVersion
75.0
application.xpcomAbi
x86_64-msvc
application.channel
release
clientId
c0ffeec0-ffee-c0ff-eec0-ffeec0ffeec0

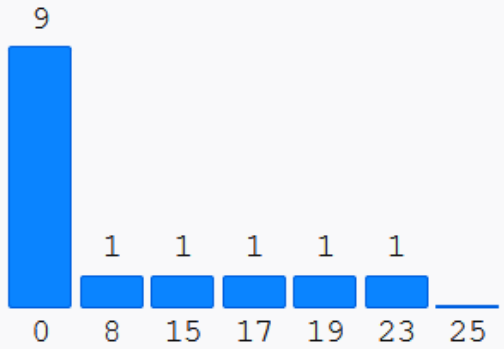

Telemetry Data
about:telemetry#environment-data-tab_system
60%
Environment Data - system
Find in Environment Data
current data
Home
General Data
Environment Data
Build
Partner
System
Settings
Profile
Experiments
Addons
Session Information
Scalars
Keyed Scalars
Histograms
Keyed Histograms
Events
Simple Measurements
Raw JSON
system
Property
Value
memoryMB
16275
virtualMaxMB
134217728
cpu.count
8
cpu.cores
4
cpu.vendor
GenuineIntel
cpu.family
6
cpu.model
158
cpu.stepping
9
cpu.l2cacheKB
256
cpu.l3cacheKB
8192
cpu.speedMHz
3600
cpu.extensions
[hasMMX, hasSSE, hasSSE2, hasSSE3, hasSSSE3, hasSSE4_1, hasSSE4_2, hasAVX, hasAVX2, hasAES]
os.installYear
2019
os.hasSuperfetch
true
os.hasPrefetch
true
os.name
Windows_NT
os.version
10.0
os.locale
en-US
os.servicePackMajor
0
os.servicePackMinor
0
os.windowsBuildNumber
18363
os.windowsUBR
752
hdd.binary.model
IntelOptane+931GBHDD
hdd.binary.revision
15.9
hdd.binary.type
HDD
hdd.profile.model
IntelOptane+931GBHDD
hdd.profile.revision
15.9
hdd.profile.type
HDD
hdd.system.model
IntelOptane+931GBHDD


Telemetry Data
about:telemetry#session-info-tab
110%
current data
Home
General Data
Environment Data
Session Information
Scalars
Keyed Scalars
Histograms
Keyed Histograms
Events
Raw JSON
Session Information
Find in Session Information
Property
Value
reason
gather-subsession-payload
revision
https://hg.mozilla.org/releases/mozilla-release/rev/6200ca9b300670ec069cdbf6e4f05e6a0bca46f1
timezoneOffset
-300
previousBuildId
null
sessionId
5dce86e2-d3ed-4c46-b933-24d8b080b34e
subsessionId
1a2e4cb5-a286-4de9-b818-382b9ca6f0bb
previousSessionId
2f329abb-d77b-4ab5-9a9f-1079c525f6db
previousSubsessionId
a365858a-cfa0-48e6-b940-bb64e2865efb
subsessionCounter
2
profileSubsessionCounter
749
sessionStartDate
2020-04-12T18:00:00.0-05:00
subsessionStartDate
2020-04-13T00:00:00.0-05:00
sessionLength
68609
subsessionLength
47044

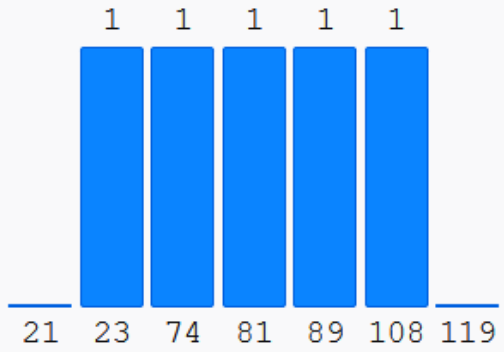
Telemetry Data

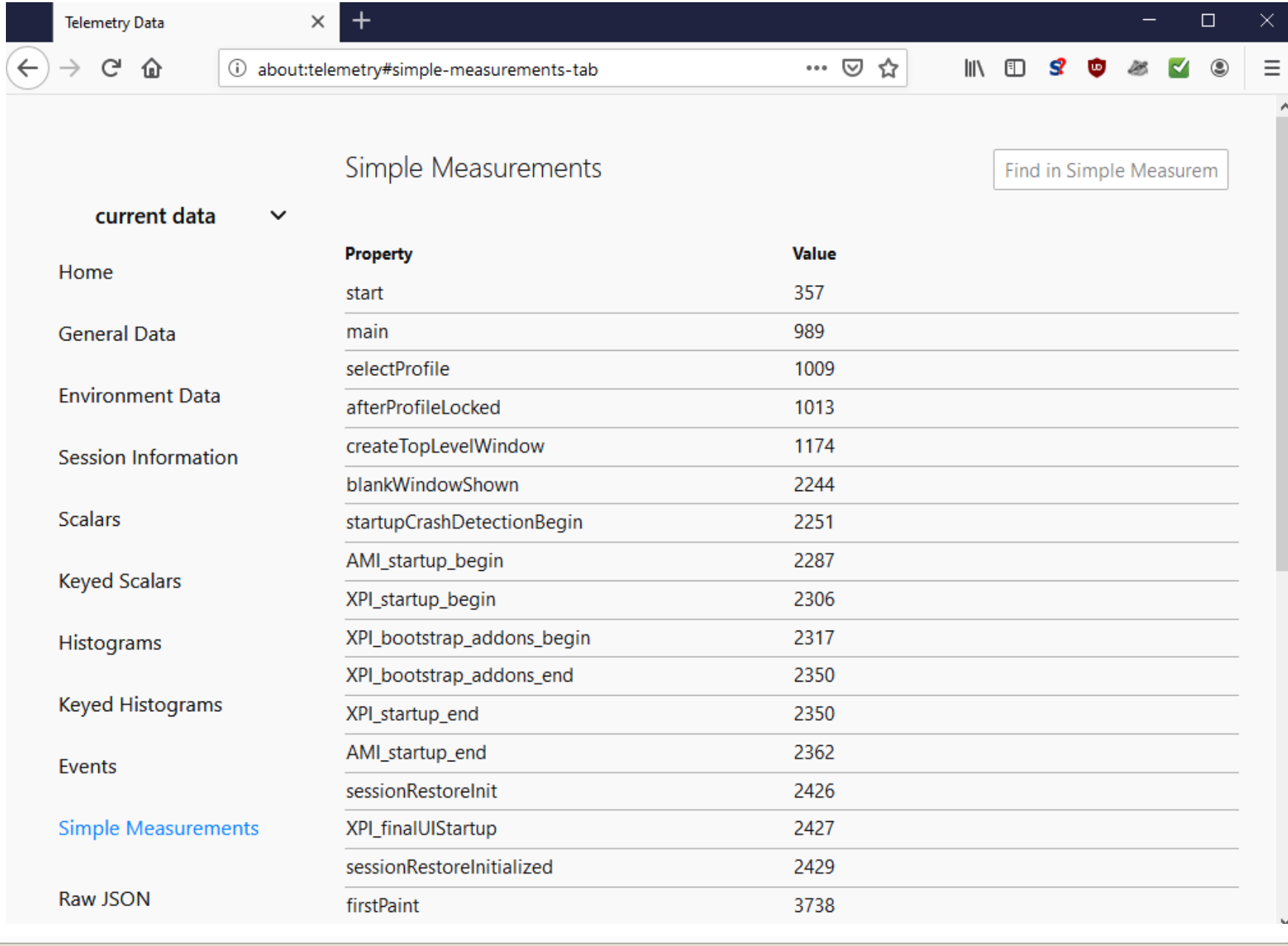
about:telemetry#keyed-histograms-tab_content 110%

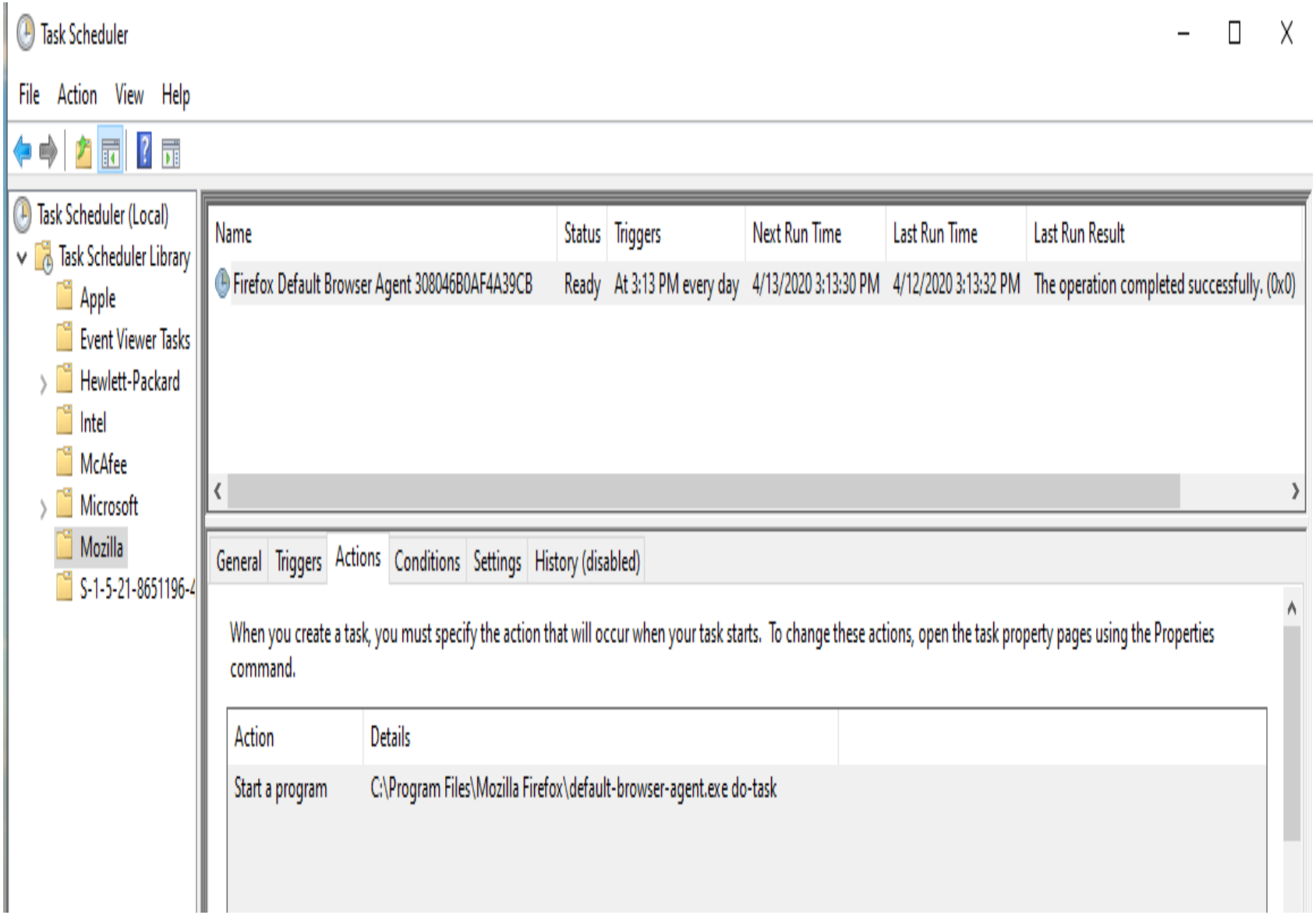
- Environment Data
- Session Information
- Scalars
- Keyed Scalars
- Histograms
- Keyed Histograms
  - Parent
  - Content
  - Extension
- Events
- Simple Measurements
- Raw JSON

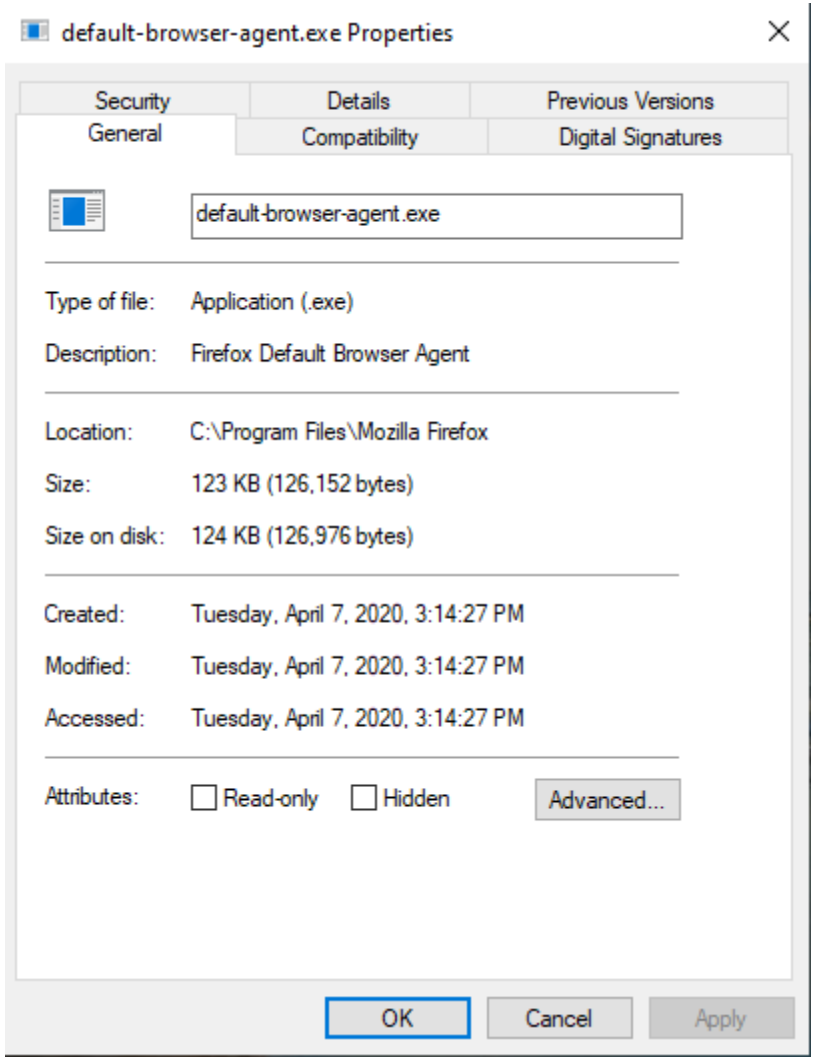


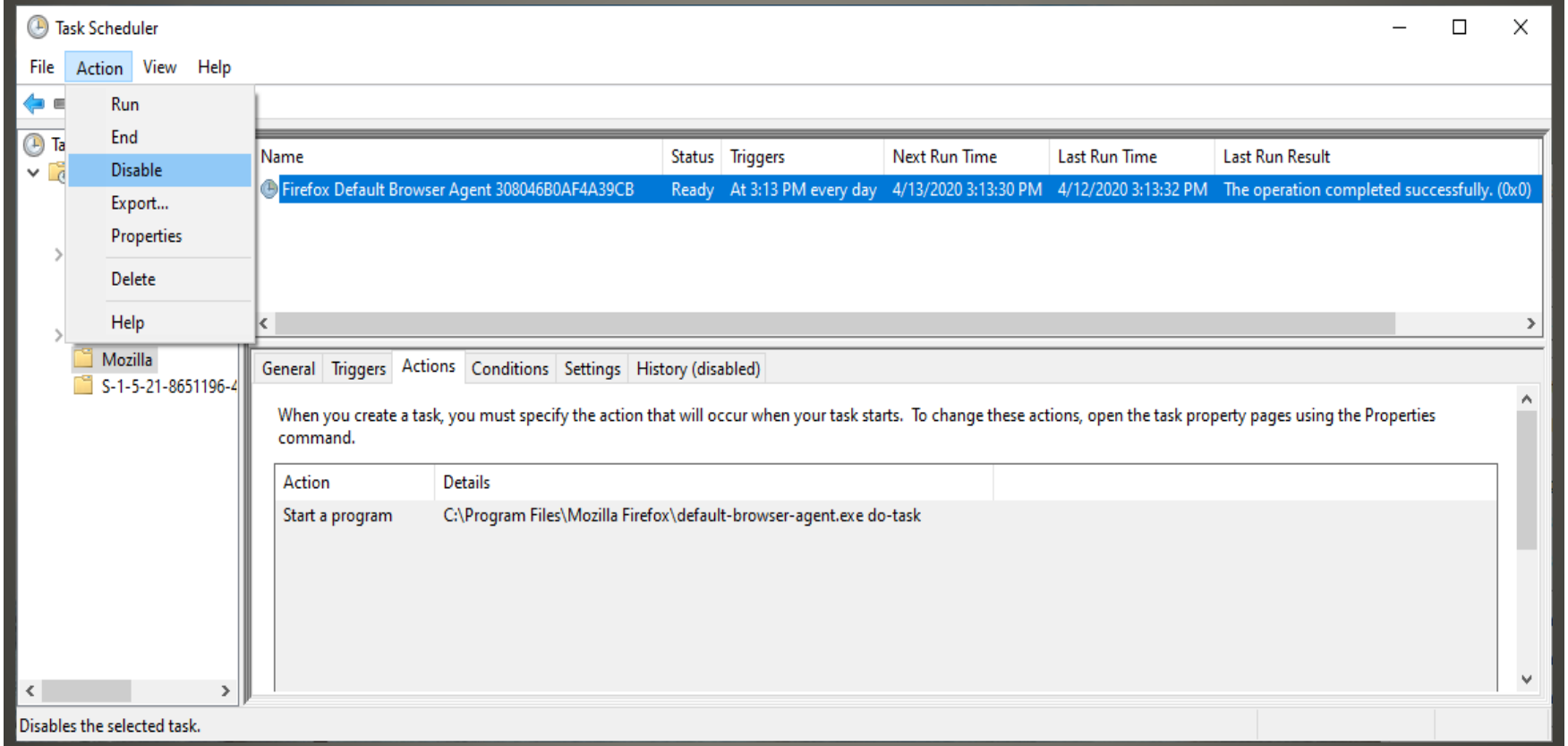
scriptsafe@protonmail.com

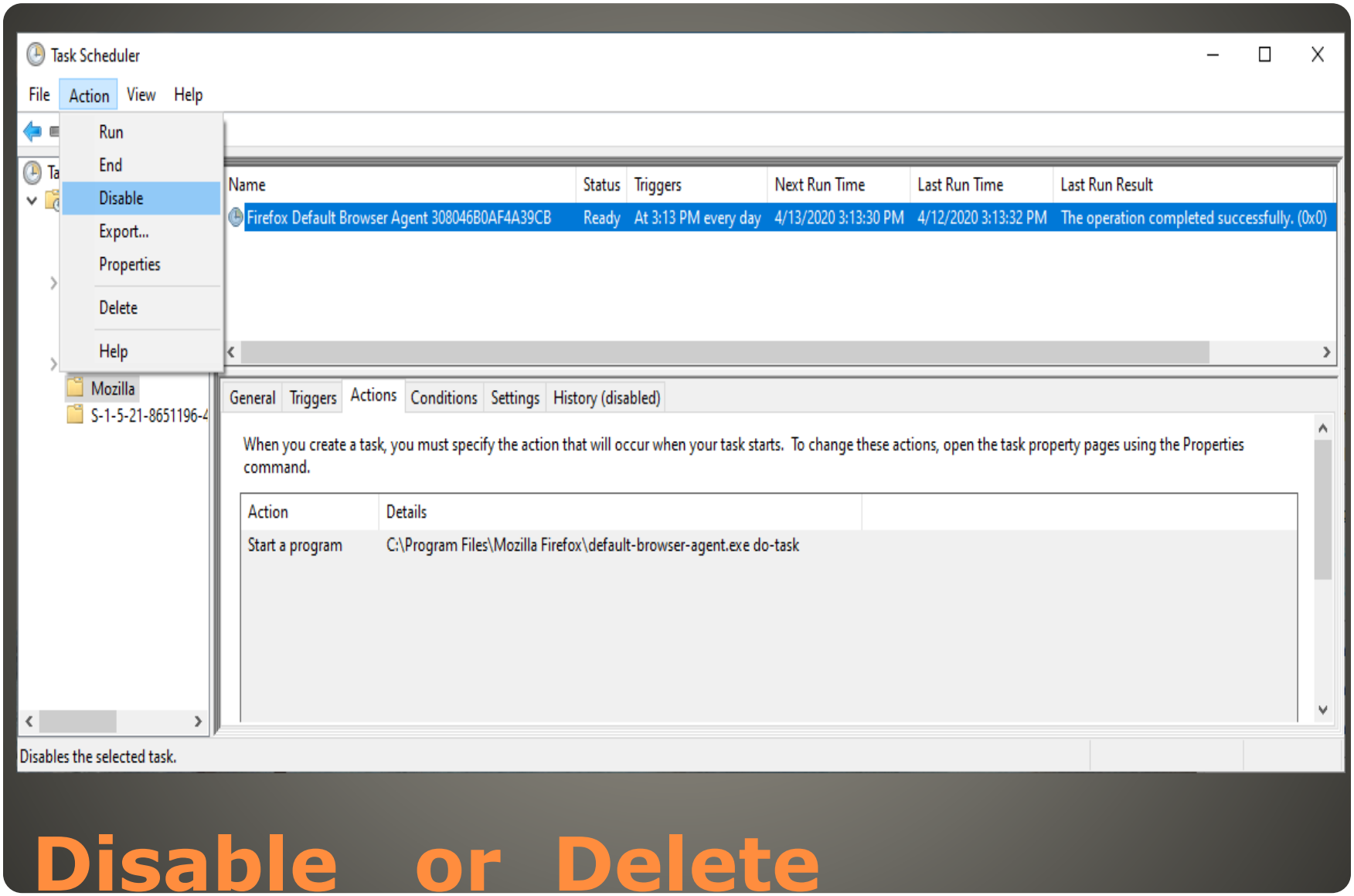



Telemetry Data
about:telemetry#simple-measurements-tab
Simple Measurements
Find in Simple Measurem
current data
Home
General Data
Environment Data
Session Information
Scalars
Keyed Scalars
Histograms
Keyed Histograms
Events
Simple Measurements
Raw JSON
Property
Value
start 357
main 989
selectProfile 1009
afterProfileLocked 1013
createTopLevelWindow 1174
blankWindowShown 2244
startupCrashDetectionBegin 2251
AMI_startup_begin 2287
XPI_startup_begin 2306
XPI_bootstrap_addons_begin 2317
XPI_bootstrap_addons_end 2350
XPI_startup_end 2350
AMI_startup_end 2362
sessionRestoreInit 2426
XPI_finalUIStartup 2427
sessionRestoreInitialized 2429
firstPaint 3738


Task Scheduler
File Action View Help
Task Scheduler (Local)
Task Scheduler Library
Apple
Event Viewer Tasks
Hewlett-Packard
Intel
McAfee
Microsoft
Mozilla
S-1-5-21-8651196-4
Name
Status
Triggers
Next Run Time
Last Run Time
Last Run Result
Firefox Default Browser Agent 308046B0AF4A39CB
Ready
At 3:13 PM every day
4/13/2020 3:13:30 PM
4/12/2020 3:13:32 PM
The operation completed successfully. (0x0)
General
Triggers
Actions
Conditions
Settings
History (disabled)
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.
Action
Details
Start a program
C:\Program Files\Mozilla Firefox\default-browser-agent.exe do-task


default-browser-agent.exe Properties
Security
Details
Previous Versions
General
Compatibility
Digital Signatures
default-browser-agent.exe
Type of file: Application (.exe)
Description: Firefox Default Browser Agent
Location: C:\Program Files\Mozilla Firefox
Size: 123 KB (126,152 bytes)
Size on disk: 124 KB (126,976 bytes)
Created: Tuesday, April 7, 2020, 3:14:27 PM
Modified: Tuesday, April 7, 2020, 3:14:27 PM
Accessed: Tuesday, April 7, 2020, 3:14:27 PM
Attributes: Read-only Hidden Advanced...
OK
Cancel
Apply


Task Scheduler
File
Action
View
Help
Run
End
Disable
Export...
Properties
Delete
Help
Name
Status
Triggers
Next Run Time
Last Run Time
Last Run Result
Firefox Default Browser Agent 308046B0AF4A39CB
Ready
At 3:13 PM every day
4/13/2020 3:13:30 PM
4/12/2020 3:13:32 PM
The operation completed successfully. (0x0)
Mozilla
S-1-5-21-8651196-4
General
Triggers
Actions
Conditions
Settings
History (disabled)
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.
Action
Details
Start a program
C:\Program Files\Mozilla Firefox\default-browser-agent.exe do-task
Disables the selected task.



Disable or Delete

Telemedicine

- Previous employer
- Many remote small staff locations
- Roll around cart
- Data at rest
- HIPPA suspended during pandemic
- Tracking/privacy
- Nuance NotPetya

- Multiple Wireless Access Points
- Hardwire sensitive components
- Use *old* devices for control
- Monitor

Home Network security

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com

QUESTIONS?