Tools PoC Report

Name: Piyush Babele

Intern ID: 386

Tool Used:

1. Mimikatz
2. Najdsi- http://www.najdi.si

🛠 Tool Name: Mimikatz

🏛 History

Mimikatz was developed by Benjamin Delpy (aka gentilkiwi) as a research project in 2007 and became widely known for its ability to extract plaintext passwords from Windows memory.

🗎 Description

Mimikatz is an open-source post-exploitation and credential-dumping tool primarily used for Windows. It can extract plaintext passwords, hashes, PINs, and Kerberos tickets from memory.

📌 What Is This Tool About?

Mimikatz allows penetration testers and attackers to demonstrate the impact of credential theft in Windows environments. It is especially useful in Red Team operations and Active Directory assessments.

☆ Key Characteristics / Features

- Extracts plaintext credentials from LSASS memory
- Dumps NTLM hashes
- Pass-the-Hash and Pass-the-Ticket support
- Kerberos ticket extraction (TGT/TGS)
- Golden & Silver Ticket attacks
- Overpass-the-Hash
- Inject and manipulate Kerberos tokens
- Works via command line or scripts
- Compatible with Windows 7 and later
- Can be compiled and obfuscated for AV evasion

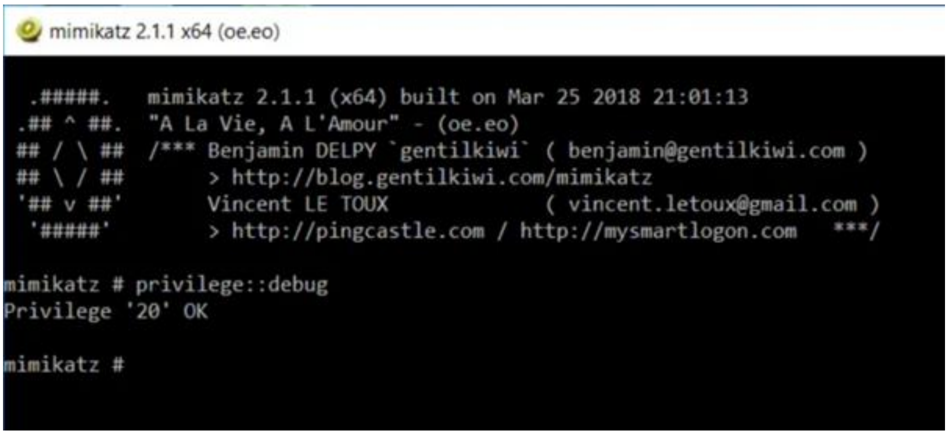
🔧 Types / Modules Available

1. `sekurlsa` – Dump credentials
2. `kerberos` – Ticket extraction
3. `crypto` – Certificate & DPAPI export
4. `token` – User impersonation
5. `privilege` – Elevation & debug rights
6. `logonpasswords` – Show all logon credentials
7. `lsadump` – LSA secrets, SAM database

🎯 How Will This Tool Help?

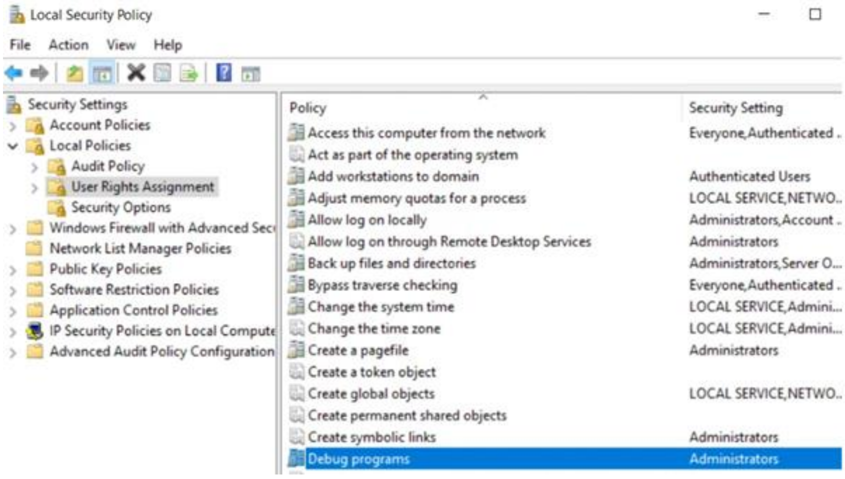
It allows the attacker (or auditor) to demonstrate credential theft risk, privilege escalation, and lateral movement capabilities within a compromised environment.

🖼 Proof of Concept (PoC) Images



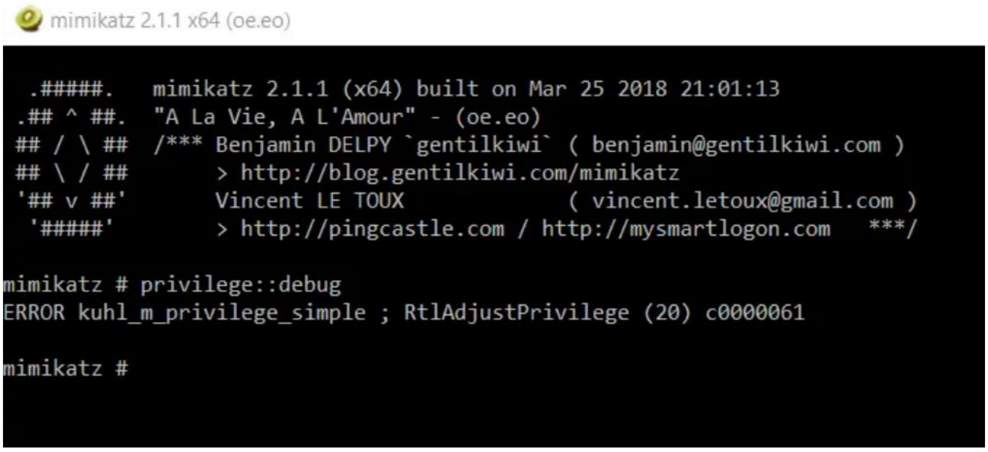
```
  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

Fig.1 Mimikatz Interface


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Access this computer from the network	Everyone,Authenticated ..
Act as part of the operating system	
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Administrators,Account ..
Allow log on through Remote Desktop Services	Administrators
Back up files and directories	Administrators,Server O...
Bypass traverse checking	Everyone,Authenticated ..
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators

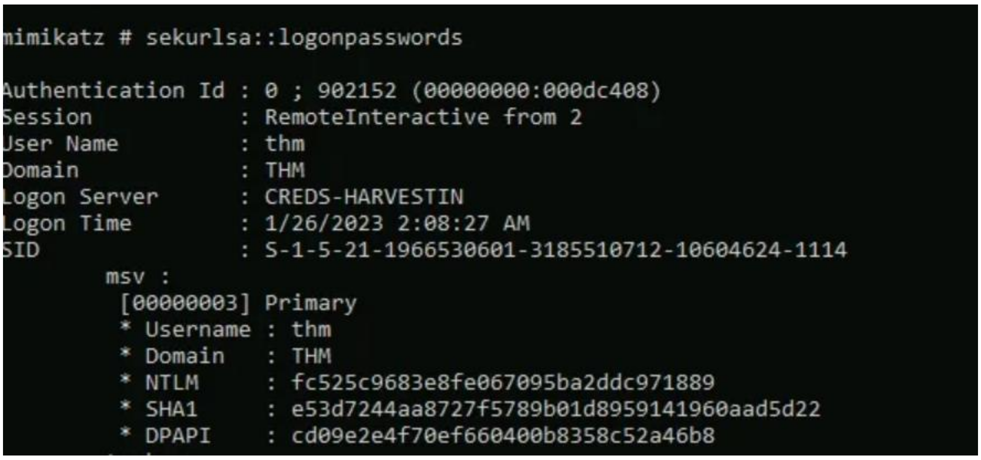
Fig.2 Debugging Privilages



mimikatz 2.1.1 x64 (oe.eo)

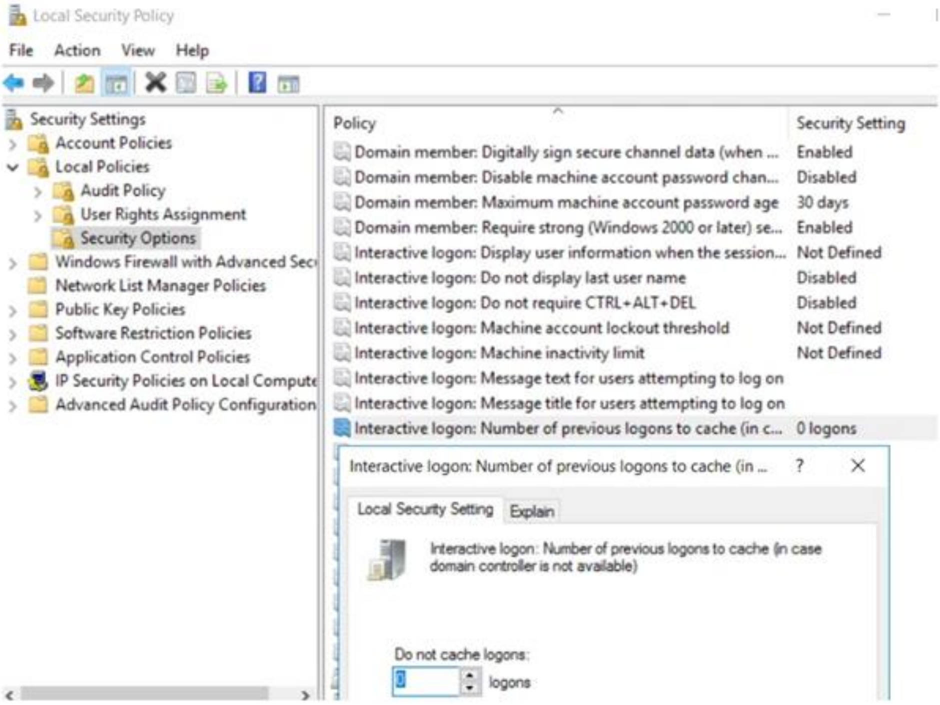
```
  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz #
```

Fig.3 `privilage::debug` *command line*



```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 902152 (00000000:000dc408)
Session           : RemoteInteractive from 2
User Name         : thm
Domain            : THM
Logon Server      : CREDS-HARVESTIN
Logon Time        : 1/26/2023 2:08:27 AM
SID               : S-1-5-21-1966530601-3185510712-10604624-1114
        msv :
         [00000003] Primary
         * Username : thm
         * Domain   : THM
         * NTLM     : fc525c9683e8fe067095ba2ddc971889
         * SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
         * DPAPI    : cd09e2e4f70ef660400b8358c52a46b8
```

Fig.4 `sekrulsa::logonpasswords` *(command for login-credentials dump)*



Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secı
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Domain member: Digitally sign secure channel data (when ...	Enabled
Domain member: Disable machine account password chan...	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) se...	Enabled
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not display last user name	Disabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in c...	0 logons

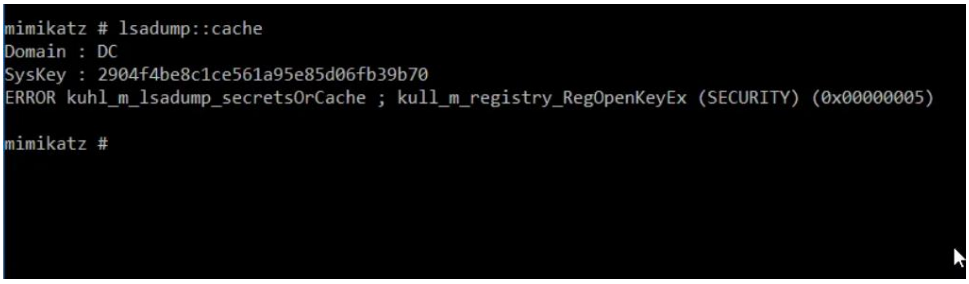
Interactive logon: Number of previous logons to cache (in ... ? ×
Local Security Setting
Explain

Interactive logon: Number of previous logons to cache (in case domain controller is not available)

Do not cache logons:

0 logons

Fig.5 Cache Logs Viewing



```
mimikatz # lsadump::cache
Domain : DC
SysKey : 2904f4be8c1ce561a95e85d06fb39b70
ERROR kuhl_m_lsadump_secretsOrCache ; kull_m_registry_RegOpenKeyEx (SECURITY) (0x00000005)

mimikatz #
```

Fig.6 `lsadump::cache` *(command for hash dumps, LSA secrets or SAM database)*

□ 15-Liner Summary

1. Open-source credential-dumping tool
2. Dumps plain text and hashed credentials
3. Extracts from LSASS and SAM
4. Supports Kerberos ticket attacks
5. Enables Golden/Silver Ticket attacks
6. Performs privilege escalation
7. Command-line interface
8. Requires debug privilege
9. Widely used in Red Team assessments
10. Bypasses weak security settings
11. Integrates with PowerShell
12. Mimics legitimate tokens
13. Works with various modules
14. Demonstrates real-world attack impact
15. Requires careful usage in legal contexts

⏱ Time to Use / Best Case Scenarios

- During Red Team assessments
- After gaining local admin/system access
- On compromised endpoints to extract credentials
- While testing Active Directory resilience

🕵 When to Use During Investigation

- During post-exploitation in Red Teaming
- Insider threat simulations
- During credential theft or lateral movement simulation
- To detect security misconfigurations in corporate AD

🧑‍💻 Best Person to Use & Required Skills

Best User: Red Team Analyst, Penetration Tester, Security Auditor

Skills Required:

- Windows OS internals understanding
- Admin/system-level access
- Knowledge of Active Directory and Kerberos
- Familiarity with post-exploitation tools
- Comfort with CLI/PowerShell scripting

▯ Flaws / Suggestions to Improve

Flaws:

- Detected easily by modern antivirus & EDR
- Requires elevated privileges
- No GUI; CLI only

Suggestions:

- Add GUI for education use
- Improve anti-detection by dynamic compilation
- Develop safe simulation mode for learning

✅ Good About the Tool

- Extremely powerful and feature-rich
- Free and open-source
- Widely accepted in Red Team workflows
- Excellent for demonstrating risks of poor credential hygiene

---

🛠 Tool Name: Najdi.si

🏛 History

Najdi.si was launched in Slovenia in 2005 by Interseek, offering Slovenian-language web search with additional features like news aggregation, business directories, and weather updates. Once popular locally, its relevance has declined with the rise of global search engines.

Description

Najdi.si is a privacy-centric, Slovenian-language search engine that offers basic web searches along with local media, phonebook, and business listings. Its minimal interface and basic features cater to casual users rather than technical or investigative professionals.

What Is This Tool About?

While Najdi.si functions as a web search engine for the Slovenian region, it does not support advanced filtering or indexing of cyber or forensic-related topics. It emphasizes privacy over powerful search capabilities, limiting its application in technical investigations.

Key Characteristics / Features

- Basic keyword-based search
- Slovenian-focused indexing
- Privacy-oriented search behavior
- Tabs include: Web, Yellow Pages, News, Weather
- No user tracking or profiling
- Clean and ad-free interface
- Lightweight, fast loading pages
- Local domain filtering (Slovenian results)
- Includes phone and business search
- Email and TV guide integration (for local users)

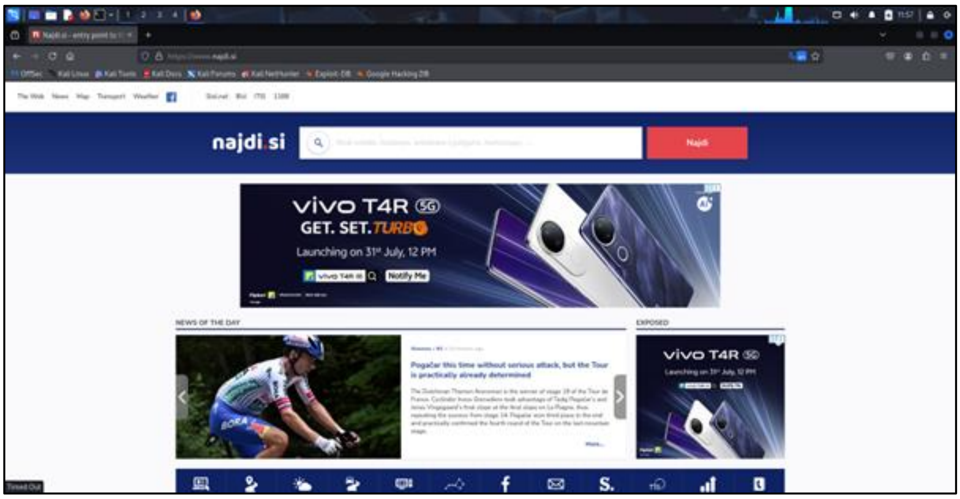
Types / Modules Available

- Web Search
- Yellow Pages (Business directory)
- News Aggregator
- Weather and TV Guide
- Traffic Guide
- Culture, The Chronicles, etc tabs

How Will This Tool Help?

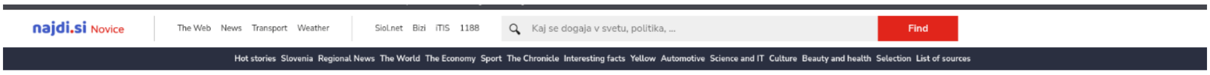
Najdi.si is best suited for simple Slovenian-language searches, such as public information lookup or neutral topic research. It is not ideal for cyber investigations or technical OSINT activities due to limited data indexing and poor coverage of relevant terms.

🖼 Proof of Concept (PoC) Images

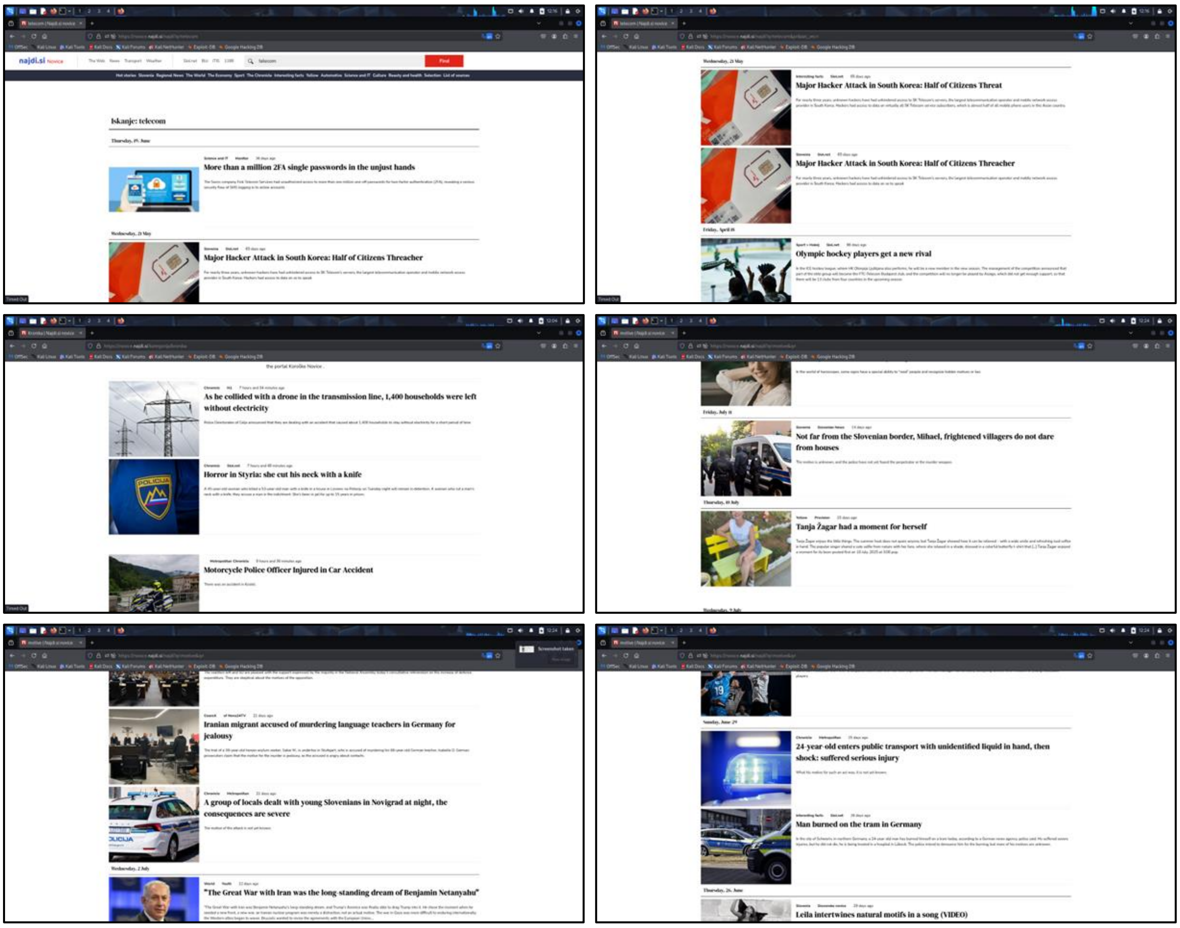


Pogačar this time without serious attack, but the Tour is practically already determined

Main Page of Najdsi Search Engine


najdi.si Novice
The Web News Transport Weather
Siol.net Bizi iTIS 1188
Kaj se dogaja v svetu, politika, ...
Find
Hot stories Slovenia Regional News The World The Economy Sport The Chronicle Interesting facts Yellow Automotive Science and IT Culture Beauty and health Selection List of sources

Search Tabs


Iskanje: telecom

Thursday, 19 June

More than a million 2FA single passwords in the unjust hands

Wednesday, 21 May

Major Hacker Attack in South Korea: Half of Citizens Threacher

Major Hacker Attack in South Korea: Half of Citizens Threat

Major Hacker Attack in South Korea: Half of Citizens Threacher

Friday, April 18

Olympic hockey players get a new rival

the portal Koroške Novice .

As he collided with a drone in the transmission line, 1,400 households were left without electricity

Horror in Styria: she cut his neck with a knife

Motorcycle Police Officer Injured in Car Accident

Friday, July 11

Not far from the Slovenian border, Mihael, frightened villagers do not dare from houses

Thursday, 10 July

Tanja Žagar had a moment for herself

Wednesday, 9 July

Iranian migrant accused of murdering language teachers in Germany for jealousy

A group of locals dealt with young Slovenians in Novigrad at night, the consequences are severe

Wednesday, 2 July

"The Great War with Iran was the long-standing dream of Benjamin Netanyahu"

Sunday, June 29

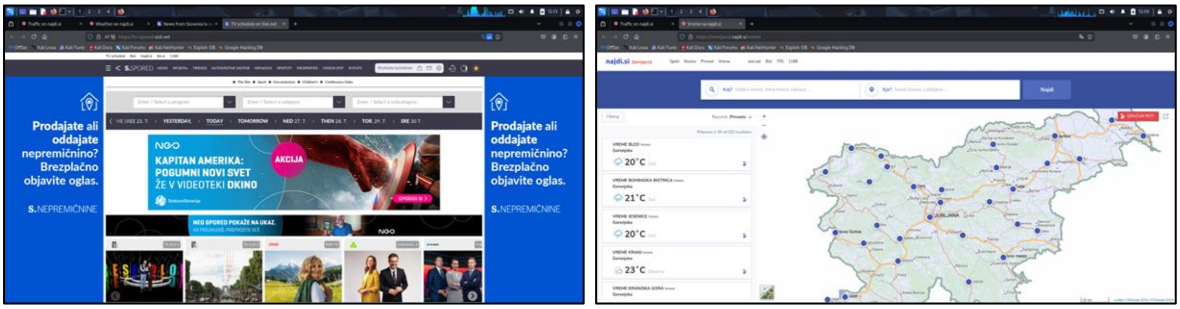
24-year-old enters public transport with unidentified liquid in hand, then shock: suffered serious injury

Man burned on the tram in Germany

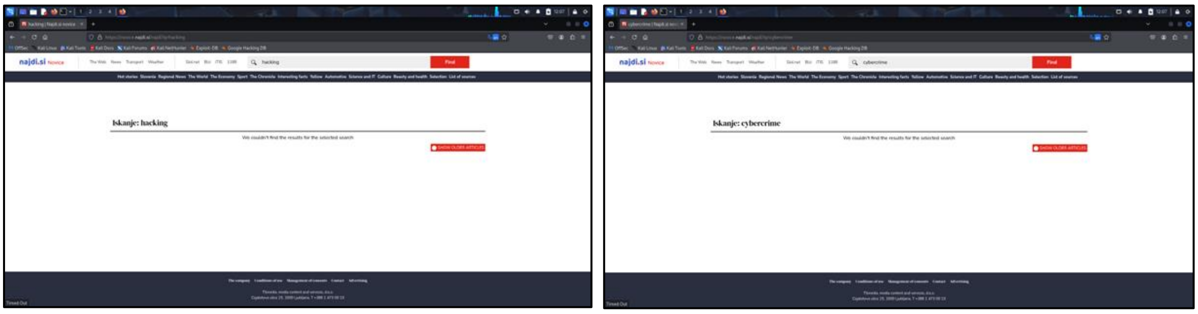
Thursday, 26. June

Leila intertwines natural motifs in a song (VIDEO)

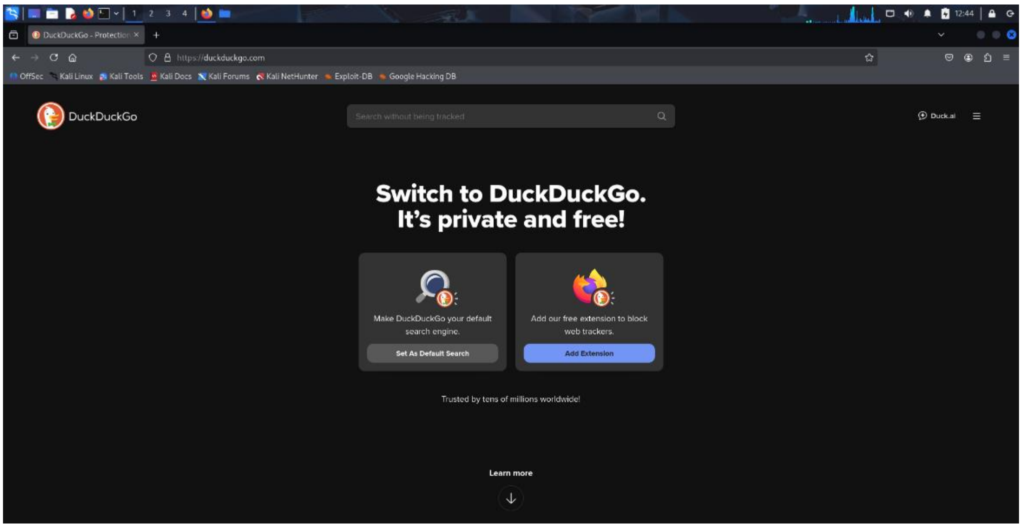
All these news related to crimes are listed in "Yellow" option below the search bar


Prodajate ali oddajate nepremičnino? Brezplačno objavite oglas.
S.NEPREMIČNINE
KAPITAN AMERIKA: POGUMNI NOVI SVET ŽE V VIDEOTEKI DOKINO
AKCIJA
najdi.si
20°C
21°C
20°C
23°C
LJUBLJANA

TV schedule and Maps


najdi.si
Iskanje: hacking
We couldn't find the results for the selected search
najdi.si
Iskanje: cybercrime
We couldn't find the results for the selected search

Direct use of words such as crime, cybercrime, hacking, etc doesn't show any result



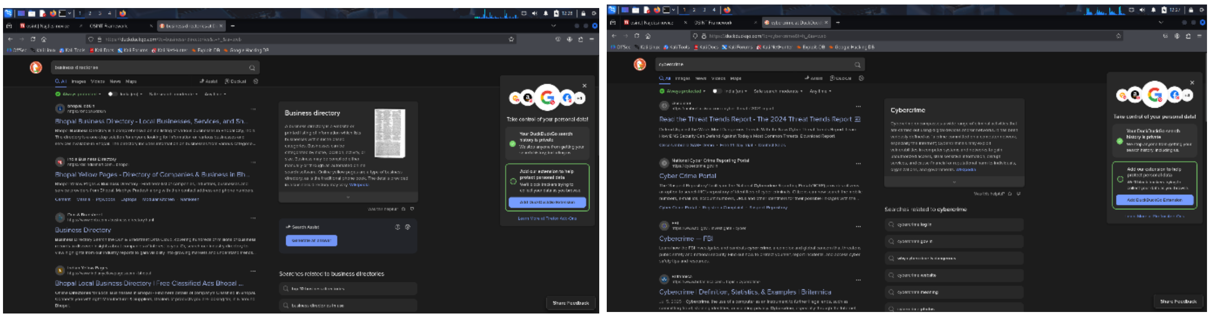
Switch to DuckDuckGo.
It's private and free!

Make DuckDuckGo your default search engine.

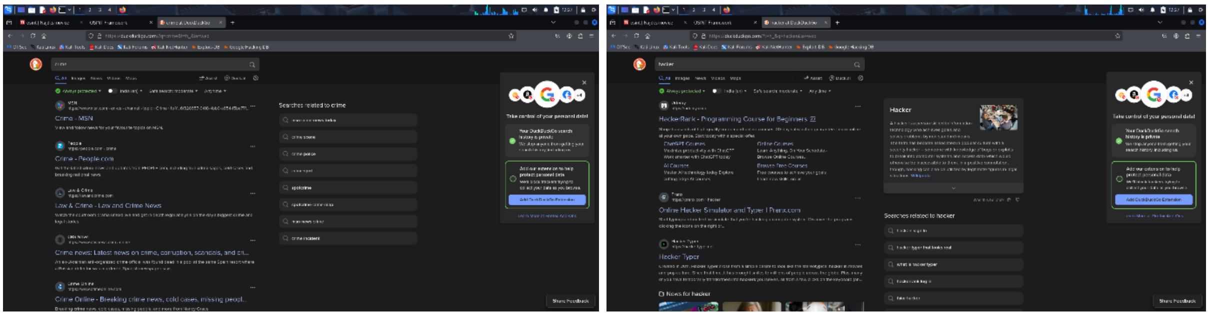
Add our free extension to block web trackers.

Trusted by tens of millions worldwide!

DuckDuckGo Search Engine (OSINT) for comparison study



Business directories & Cybercrime search results



Crime & Hacker search results

□ 15-Liner Summary

1. Najdi.si is a privacy-based search engine.
2. It was tested for cyber-related keywords.
3. Words like "crime", "cybercrime", "hacking" gave no useful results.
4. DuckDuckGo gave accurate, relevant results.
5. Najdi.si showed some crime terms in the "Yellow" tab.
6. No direct cybercrime or hacking info was found.
7. Most results were generic or unrelated.
8. DuckDuckGo outperformed in depth and accuracy.
9. Najdi.si lacks strong coverage of technical topics.
10. Its clean UI offers no filters or tools.
11. Privacy seems prioritized over result quality.
12. Useful for basic or neutral topics only.
13. Not suitable for digital forensics research.
14. Limited use in OSINT or cyber investigations.
15. Overall, Najdi.si is private but not practical.

⏱ Time to Use / Best Case Scenarios

- For basic, regional web searches
- When language-specific lookup (Slovenian) is required
- For verifying local news or listings
- In non-technical investigations

🕵 When to Use During Investigation

- Public information lookup in Slovenia
- Surface-level searches of business or people
- Only when global search engines are blocked
- For general or non-sensitive research

🧑‍💻 Best Person to Use & Required Skills

Best User: Regional journalists, local researchers, or privacy-focused users

Skills Required:

- Familiarity with Slovenian language
- Basic search literacy
- No technical or forensic background needed

▯ Flaws / Suggestions to Improve

Flaws:

- Poor indexing of cyber, hacking, or forensics content
- Lacks filtering, search operators, or metadata tools
- Results are often irrelevant or outdated

Suggestions:

- Expand search indexing to include global sources
- Add advanced search filters
- Enable multilingual support and cyber topic tagging

✅ Good About the Tool

- Fast and minimalistic
- Protects user privacy
- Works well for neutral/local topics
- No to minimal ads, clean interface
- Lightweight for low-bandwidth use