(S//SI//REL) User-agents: Why and How and How to

The overall classification of this briefing to TOP SECRET//COMINT//REL TO USA, FVEY

– S2I61

July 2010

Derived From
NSA/CSSM 1-52
Dated 20070108
Declassify on: 20320108

Agenda

- WHY: Learn why we care about user agents (UAs)
- HOW: Learn how to read a user-agent
- HOW TO: (get it?) Learn how to use user-agents in our tools

WHY?

What is a User-Agent?

A user-agent is a string which lets websites know your:

- type of web-browser or application
- Operating System
- Security settings or permissions
- Versions of relevant programs (media, java, etc.)
- Etc. (Language settings, ad-ware)

Why would I want to give a website that?

- Compatibility
- Specific Website Features
- Security permissions

User-Agents Can

- Link a target's "selected" activity to their unselected web-browsing
- Create a tentative link between targets that have the same user-agent
- Identify CNE opportunities

BUT...

User-Agents Also

- Can vary from very unique to extremely common
- Change with software updates
- Only identify the web-browser
  - 2 web-browsers = 2 user-agents
- Can’t be trusted...

Who started this nonsense?

A History Lesson

The Great Browser Wars

Back...in the 20th Century!

Before Now but After What is Below

Remember Frames?

- Netscape's new fancy web-browser support them!
- The original "web-browser" Mosaic did not
- And so began browser "sniffing"

Worthless Trivia!

- Mosaic was the first web-browser to embed images with text
- It supported FTP, Usenet, and Gopher!
- Its web-browser competitors at the time were Erwise and ViolaWWW

The Great Internet Explorer Hoax

Ever wonder why so many user agents start with “Mozilla” but aren’t Firefox?

Internet Explorer fools us all

- When Internet Explorer was released it did frames too!
- But since its user-agent didn't say so, no websites would send their super cool frames version to the IE users

What to do?

LIE, of course!

Internet Explorer starts to spoof

- Internet Explorer changed its user agent starting their user agent with Mozilla/1.22
- Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

And it continues to this very day...

The How...

Three Basic Pieces of the UA

Mozilia/1.22 (compatible; MSIE 2.0; Windows 95)

Mozilla/1.22

Part 1: The Netscape Historical Token

- Appears in primarily Mozilla Firefox, Google Chrome, and MSIE browsers
  - Modern Version: Mozilla 4.0 or Mozilla 5.0
  - Does not indicate a target uses “Mozilla Firefox”

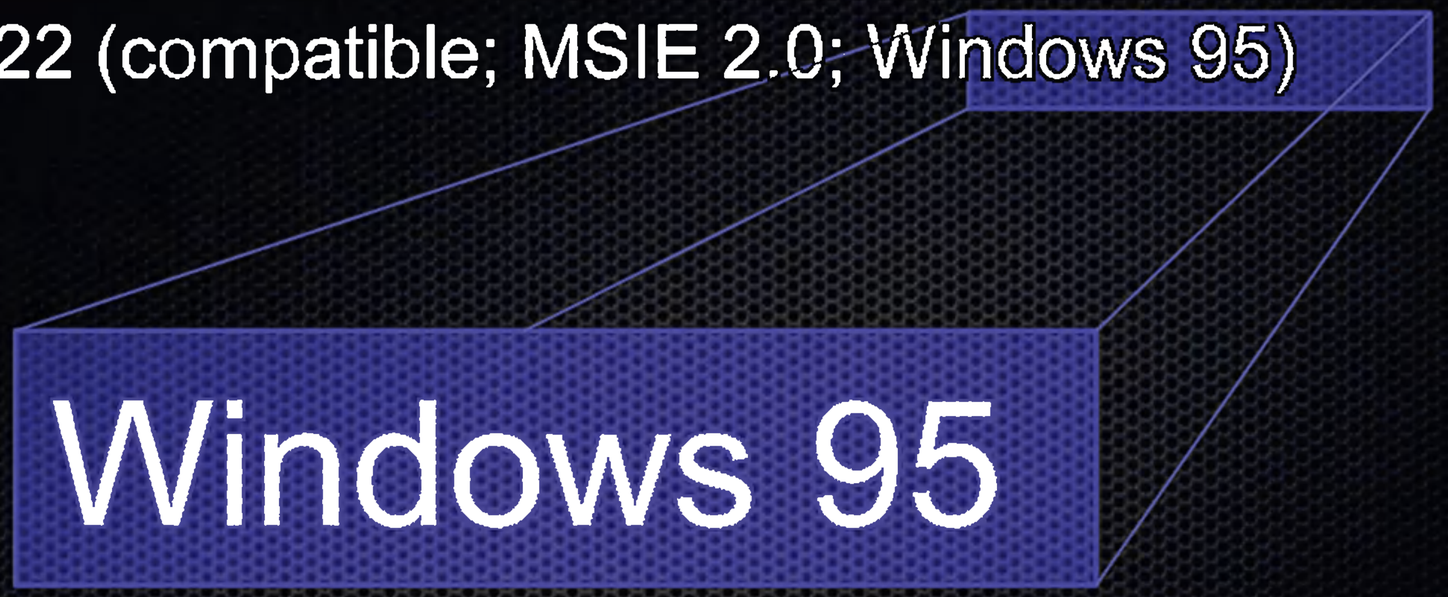
Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)

MSIE 2.0

Part 2: The Web Browser Identifier

- Appears in generally all user-agents
- Not always in the same place, but usually self explanatory
  - Opera X.X = Opera
  - Firefox X.X = Firefox
  - Safari X.X= Safari
  - Chrome X.X Safari X.X = Google Chrome

Mozilla/1.22 (compatible; MSIE 2.0; Windows 95)



Part 3: The Operating System Token

- Appears in basically all HTTP user-agent strings
  - Examples:
    - Windows NT 6.1 = Windows Version 7
    - Windows NT 6.0 = Windows Vista
    - Windows NT 5.2 = Windows XP 64bit
    - Windows NT 5.1 = Windows XP
    - Windows NT 4.0 actually equals Windows NT 4.0

Other operating systems UAs

- Mobile
  - MAC OS X
- Linux
  - Linux i686
  - Free BSD

Game Consoles

- Opera/9.30 (Nintendo Wii; U; 2047-7; en)
- Mozilla/5.0 (Playstation 3; 2.00)
- PSP (PlayStation Portable); 2.00

Mobile User Agents

- Usually self-explanatory
  - Iphone
  - Ipad
  - Blackberry
  - Android
- Mobile user agents also usually give you the phone model (Read: IMEI correlation opportunities)

Ever wonder what that was?

- Gecko: a rendering engine used by Firefox and others
- AppleWebkit: Apple's version of KHTML rendering engine used in Safari and Chrome most commonly
- Presto : the "core" of the Opera platform suite

Ever Wonder Contd.

- .NET CLR is the .NET Framework version
- SV1 is an artifact created by MSIE 6.0 to make its security better
- Win64 can indicate that the system is running a 64 bit processor

Ever Wonder... One more

Many web browsers will also have an “encryption strength” marker

U = USA (128 bit encryption)

I = International (40 bit encryption)

N = No encryption (Woo!)

Most Browsers nowadays come with a U

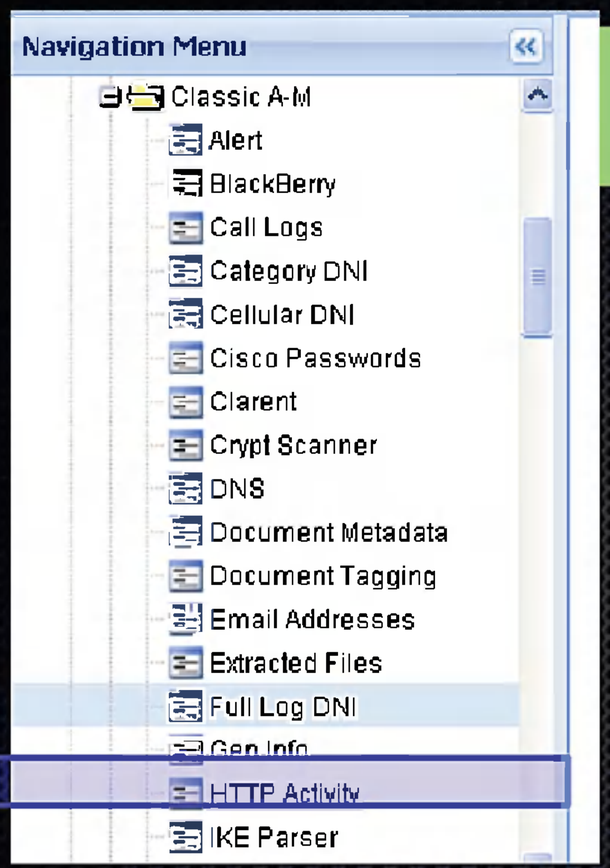
Since the USG no longer requires encryption changes for international usage.

Your target's user-agents can shorten and lengthen!

- Each website may require different information
- Longer user-agents may have various rendering engine, java versions, and language settings
- If you see a shortened or longer version of a UA close to your targets logins. Check it out! Carefully...

The How To...

Querying in Xkeyscore



Browser: Mozilla 5.0*

Remember:
Since Xkeyscore no longer supports leading wildcards you need to be specific with your User-Agent

A User-agent alone is not a strong query
Time Frame, Active IP,
Country, etc. all will help make your query compliant

Browser
Mozilla:5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit.533.4 (KHTML, like Gecko) Chrome:5.0.375.99 Safari:533.4

Uniqueness – When to use a User-Agent

Reports View Filters

Browser	Geo Info
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	

- Sort Ascending
- Sort Descending
- Filters
- Color By
- Group By
- Histogram
- Pivot Data
- Histogram Grid
- Show/Hide...
- AutoFit Column Width

Results of an IP-based search for a target

Histogram Grid

Page 1 of 1 | Clear Selection | Export

Filter	Browser	Count
	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	6
	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	6

Low Number of users and traffic volume as well as only 2 User-agents

Verdict: Probably reliable

More User = More Problems

Browser	Count
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	6
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648;	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729;	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB0.0; .NET CLR 2.0.50727; AskTB5.6)	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.5)	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.5; .NET CLR 2.0.50727)	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.5; InfoPath.2)	2
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.5; InfoPath.2; .NET CLR 2.0.50727; .NET	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 3.0.	1
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)	1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)	6
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)	1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; FunWebProducts; AskTbPTV/5.8.0.12304)	1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; .NET CLR 1.1.4322)	1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; IEMB3; IEMB3)	1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727	1
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; InfoPath.2; .NET CLF	2

Reliability of correlating your target's browser to his web-activity plummets due to User-agent variations and the threat of multiple users.

At this point, cookie and TDI correlation are necessary. User-agents can not be used by themselves.

Common Sense Helps

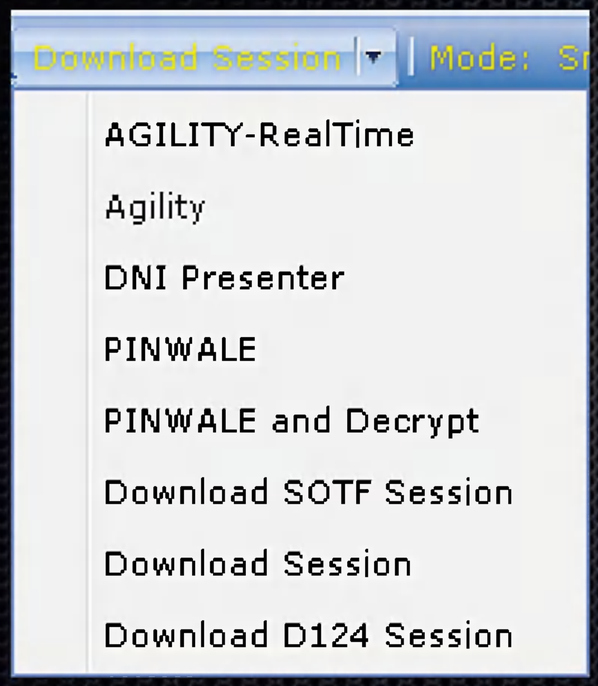
Never assume because a User-agent is complicated that it is unique

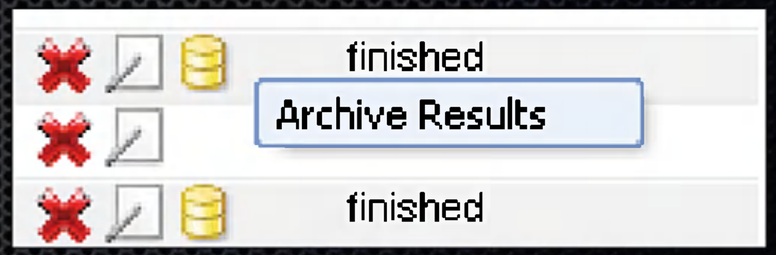
- Example:
- Mozilla 5.0 (Windows; U; Windows NT 6.1; en-US) AppleWebKit/534.3(KHTML, like Gecko) Chrome/6.0.464.0 Safari/534.3

- This is the standard user agent for **EVERYONE** with an updated Chrome browser using Windows 7.

Xkeyscore Storage

Push to Pinwale or Archive Results





Pinwale

Fields to add to Metadata View

AppProc Active User

User Agent
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) ...

Generally speaking, the User Agent listed belongs to the selector in the Active User column (if populated)

Add a User-Agent to a compliant query

Fielded Search Form

1. Put in the User Agent that is being search for into the CONTENT_META field under the fielded search form.

KEYWORDS [ ] and

cs=ISO8859_1 ((("Opera Mini")))

CONTENT_META [Opera Mini] between tags [UserAgent] and

Smart Form/ Native Query

```
Native, cs=ISO8859_1 ( (content_meta=((((("Opera Mini")) between \<UserAgent and \/UserAgent ))) )
```

```
(content_meta=((((("Opera Mini")) between \<UserAgent and \/UserAgent )))
```

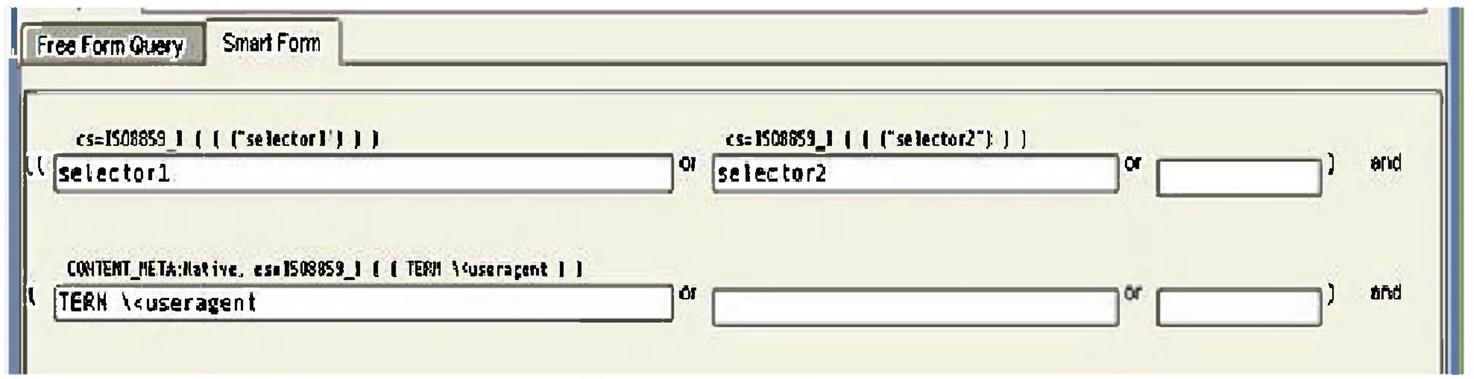
Not sure the specific User-Agent?

1. Add the following syntax to your query:

```
\TERM \<yourfield here (E.G. \TERM \<useragent )
```

2. Apply Native to the field

3. Apply the content_meta document zone to the field.



(TS//SI//REL) This query basically ensures that a certain field exists in each result thus removing all the content not relevant to your query.

User-Agent Manipulation

- The best for last
  - User-agents can completely be changed or not included by the user!
    - By Firefox Plugin
    - By Browser settings (Opera)
    - Outside programs (TOR Button)
  - These programs allow users to have a different user agent for each session!

Questions??

- Contact Info: [redacted]@nsa.ic.gov
- Website on the High-Side:
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Lots of great stuff in open source as well!
- http://www-archive.mozilla.org/build/user-agents-strings.html

Got a Tech Problem?

Have a random SIGDEV question?

Need help with a target using new tech to communicate?

Need help developing an accurate collateral description of a technology?

Want help developing Xkeyscore fingerprints for a weird target behavior?

Let us know : DL S2I61_all