

# Hello, what's your name?

*An overview of Wireshark's name resolution options*

*(and it is not only for IP addresses!)*

**Sake Blok**

*Relational therapist for computer systems*

sake.blok@SYN-bit.nl



**SYN-bit**  
deep traffic analysis



# \$ whoami



**SYN-bit**  
deep traffic analysis





# We are getting off on the wrong foot ;-)



In computer systems, **name resolution** refers to the retrieval of the underlying numeric values corresponding to computer hostnames, account user names, group names, and other named entities.

***But Wireshark shows numbers and we want names!!!***





# It's simple, right? Just turn it on!



View Go Capture Analyze Statistics Telephony Wireless Tools

filtered.pcapng — using p

- ✓ Main Toolbar
- ✓ Filter Toolbar
- ✓ Status Bar
- Full Screen
- LAN
- ✓ Packet List
- ✓ Packet Details
- ✓ Packet Bytes
- Packet Diagram
- Time Display Format
- Name Resolution**
  - Edit Resolved Name
  - ✓ Resolve Physical Addresses
  - ✓ Resolve Network Addresses
  - ✓ Resolve Transport Addresses
- Zoom
- Expand Subtrees
- Collapse Subtrees
- Expand All

Frame 17: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface unknown, id 0

Ethernet II, Src: x201.local (f0:de:f1:58:72:b5), Dst: VMware\_b0:c9:1c (00:0c:29:b0:c9:1c)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112

Internet Protocol Version 4, Src: x201.local (10.0.112.103), Dst: ns.SYN-bit.voip (10.0.103.1)

User Datagram Protocol, Src Port: 52236 (52236), Dst Port: domain (53)

???

No.	Time	VLAN	HW-src	HW-dst	Source	Destination	sport	dport	Protocol	Length	Info
13	21.130382248	1112	x201.local	Broadcast	0.0.0.0	255.255.255.255	bootpc	bootps	DHCP	338	DHCP Request - Transaction ID 0xe6744837
14	21.135129736	1112	VMware_b0:c9:1c	x201.local	10.0.112.254	x201.local	bootps	bootpc	DHCP	350	DHCP ACK - Transaction ID 0xe6744837
17	21.218529472	1112	x201.local	VMware_b0:c9:1c	x201.local	ns.SYN-bit.voip	52236	domain	DNS	108	Standard query 0x70b2 A connectivity-check.ubuntu.com OPT
18	21.219515064	1112	VMware_b0:c9:1c	x201.local	ns.SYN-bit.voip	x201.local	domain	52236	DNS	156	Standard query response 0x70b2 A connectivity-check.ubuntu.com
19	21.219527784	1112	x201.local	VMware_b0:c9:1c	x201.local	ns.SYN-bit.voip	35699	domain	DNS	108	Standard query 0x4501 AAAA connectivity-check.ubuntu.com OPT
20	21.220003784	1112	VMware_b0:c9:1c	x201.local	ns.SYN-bit.voip	x201.local	domain	35699	DNS	169	Standard query response 0x4501 AAAA connectivity-check.ubuntu.com
22	21.223418992	1112	x201.local	VMware_b0:c9:1c	x201.local	ns.SYN-bit.voip	49190	domain	DNS	108	Standard query 0xfa9a AAAA connectivity-check.ubuntu.com OPT
23	21.223854680	1112	VMware_b0:c9:1c	x201.local	ns.SYN-bit.voip	x201.local	domain	49190	DNS	169	Standard query response 0xfa9a AAAA connectivity-check.ubuntu.com





# Ignorance is bliss?

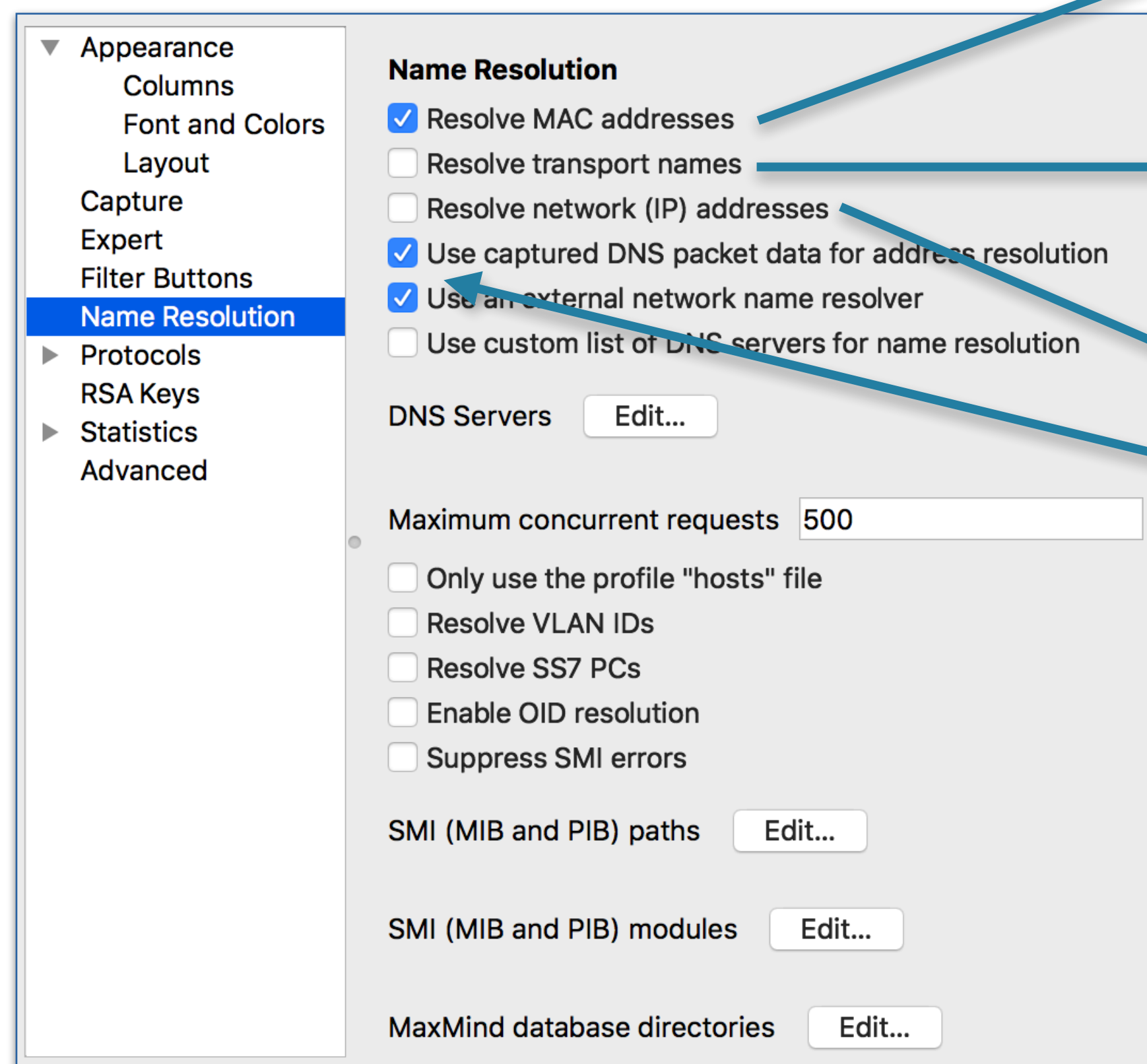


<https://flic.kr/p/8xhk74>





# By default:



The image shows the 'Name Resolution' settings panel in Wireshark. The left sidebar contains a tree view with 'Name Resolution' selected. The main panel has the following settings:

- Name Resolution**
  - Resolve MAC addresses
  - Resolve transport names
  - Resolve network (IP) addresses
  - Use captured DNS packet data for address resolution
  - Use an external network name resolver
  - Use custom list of DNS servers for name resolution
- DNS Servers
- Maximum concurrent requests
- Only use the profile "hosts" file
- Resolve VLAN IDs
- Resolve SS7 PCs
- Enable OID resolution
- Suppress SMI errors
- SMI (MIB and PIB) paths
- SMI (MIB and PIB) modules
- MaxMind database directories

Uses: **manuf** file in the **Global Configuration** directory

Uses: **services** file in the **Global Configuration** directory

Uses: **captured (m)DNS packets** and **external reverse lookups**





# But what if?



- The customer has an internal DNS server and you view the capture without access to it?
- The capture file will be viewed in the future and the DNS entries have changed?
- You want to give names to specific IPs
- You have some custom services on specific ports
- You want to see VLAN names instead of numbers
- You want to see GeolP information
- You want to see SNMP Object Names



# Many sources of naming info



- Static files (hosts/ethers/mmdb files/MIB files/etc)
  - In system files, global preferences, default personal preferences and/or a specific configuration profile
- Captured packets
  - From (forward) mDNS/DNS lookups
- External resolvers
  - Reverse lookups through DNS servers
- PCAPNG name resolution blocks
- Hardcoded in Wireshark's sourcecode
- Manually resolved names
- "Unknown" / future sources?





# File locations (Windows/Linux)



About Wireshark

Wireshark Authors Folders Plugins Keyboard Shortcuts Acknowledgments License

Filter by path

Name	Location	Typical Files
"File" dialogs	<a href="#">C:\Users\Beheer\Documents\</a>	capture files
Temp	<a href="#">C:\Users\Beheer\AppData\Local\Temp</a>	untitled capture files
Personal configuration	<a href="#">C:\Users\Beheer\AppData\Roaming\Wireshark</a>	dfilters, preferences, ethers, ...
Global configuration	<a href="#">C:\Program Files\Wireshark</a>	dfilters, preferences, manuf, ...
System	<a href="#">C:\Program Files\Wireshark</a>	ethers, ipxnets
Program	<a href="#">C:\Program Files\Wireshark</a>	program files
Personal Plugins	<a href="#">C:\Users\Beheer\AppData\Roaming\Wireshark\plugins\3.4</a>	binary plugins
Global Plugins	<a href="#">C:\Program Files\Wireshark\plugins\3.4</a>	binary plugins
Personal Lua Plugins	<a href="#">C:\Users\Beheer\AppData\Roaming\Wireshark\plugins</a>	lua scripts
Global Lua Plugins	<a href="#">C:\Program Files\Wireshark\plugins</a>	lua scripts
Personal Extcap path	<a href="#">C:\Users\Beheer\AppData\Roaming\Wireshark\extcap</a>	Extcap Plugins search path
Global Extcap path	<a href="#">C:\Program Files\Wireshark\extcap</a>	Extcap Plugins search path
MaxMind DB path	<a href="#">C:\ProgramData\GeoIP</a>	MaxMind DB database search path
MaxMind DB path	<a href="#">C:\GeoIP</a>	MaxMind DB database search path
MIB/PIB path		SMI MIB/PIB search path

OK

About Wireshark

Wireshark Authors Folders Plugins Keyboard Shortcuts Acknowledgments License

Filter by path

Name	Location	Typical Files
"File" dialogs		capture files
Temp	<a href="#">/tmp</a>	untitled capture files
Personal configuration	<a href="#">/home/sake/.config/wireshark</a>	dfilters, preferences, ethers, ...
Global configuration	<a href="#">/usr/share/wireshark</a>	dfilters, preferences, manuf, ...
System	<a href="#">/etc</a>	ethers, ipxnets
Program	<a href="#">/usr/bin</a>	program files
Personal Plugins	<a href="#">/home/sake/.local/lib/wireshark/plugins/3.2</a>	binary plugins
Global Plugins	<a href="#">/usr/lib/x86_64-linux-gnu/wireshark/plugins/3.2</a>	binary plugins
Personal Lua Plugins	<a href="#">/home/sake/.local/lib/wireshark/plugins</a>	lua scripts
Global Lua Plugins	<a href="#">/usr/lib/x86_64-linux-gnu/wireshark/plugins</a>	lua scripts
Personal Extcap path	<a href="#">/home/sake/.config/wireshark/extcap</a>	Extcap Plugins search path
Global Extcap path	<a href="#">/usr/lib/x86_64-linux-gnu/wireshark/extcap</a>	Extcap Plugins search path
MaxMind DB path	<a href="#">/usr/share/GeoIP</a>	MaxMind DB database search path
MaxMind DB path	<a href="#">/var/lib/GeoIP</a>	MaxMind DB database search path
MaxMind DB path	<a href="#">/usr/share/GeoIP</a>	MaxMind DB database search path
MaxMind DB path	<a href="#">/var/lib/GeoIP</a>	MaxMind DB database search path
MIB/PIB path		SMI MIB/PIB search path

OK





# File locations (MacOS)



Filter by path

Name	Location	Typical Files
"File" dialogs	<a href="#">/Users/sake/</a>	capture files
Global Extcap path	<a href="#">/Applications/Wireshark-3.5.0.app/Contents/MacOS/extcap</a>	Extcap Plugins search path
Global Lua Plugins	<a href="#">/Applications/Wireshark-3.5.0.app/Contents/PlugIns/wireshark</a>	lua scripts
Global Plugins	<a href="#">/Applications/Wireshark-3.5.0.app/Contents/PlugIns/wireshark/3-5</a>	binary plugins
Global configuration	<a href="#">/Applications/Wireshark-3.5.0.app/Contents/Resources/share/wireshark</a>	dfilters, preferences, manuf, ...
MIB/PIB path		SMI MIB/PIB search path
MaxMind DB path	<a href="#">/usr/share/GeoIP</a>	MaxMind DB database search path
MaxMind DB path	<a href="#">/var/lib/GeoIP</a>	MaxMind DB database search path
Personal Extcap path	<a href="#">/Users/sake/.config/wireshark/extcap</a>	Extcap Plugins search path
Personal Lua Plugins	<a href="#">/Users/sake/.local/lib/wireshark/plugins</a>	lua scripts
Personal Plugins	<a href="#">/Users/sake/.local/lib/wireshark/plugins/3-5</a>	binary plugins
<b>Personal configuration</b>	<a href="#">/Users/sake/.config/wireshark</a>	<b>dfilters, preferences, ethers, ...</b>
Program	<a href="#">/Applications/Wireshark-3.5.0.app/Contents/MacOS</a>	program files
System	<a href="#">/etc</a>	ethers, ipxnets
Temp	<a href="#">/var/folders/j8/x8jn12nd2bqd0330ts6tcp7w0000gn/T/</a>	untitled capture files
macOS Extras	<a href="#">/Applications/Wireshark-3.5.0.app/Contents/Resources/Extras</a>	Extra macOS packages

OK





# Name Resolution Deepdive



```
▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)
```

The image shows the Name Resolution settings panel in Wireshark. The left sidebar contains a tree view with 'Name Resolution' selected. The main panel has the following settings:

- Resolve MAC addresses
- Resolve transport names
- Resolve network (IP) addresses
- Use captured DNS packet data for address resolution
- Use an external network name resolver
- Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

- Only use the profile "hosts" file
- Resolve VLAN IDs
- Resolve SS7 PCs
- Enable OID resolution
- Suppress SMI errors

SMI (MIB and PIB) paths

SMI (MIB and PIB) modules

- MaxMind database directories



# VLAN name resolution



- disabled by default
- "vlans" files
  - gives individual VLAN ID's a name
  - manually edited
    - ▶ located in configuration profile
    - ▶ located in default profile

```
▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)
```

The image shows the 'Name Resolution' settings panel in Wireshark. On the left is a sidebar with a tree view containing: Appearance, Columns, Font and Colors, Layout, Capture, Expert, Filter Buttons, Name Resolution (highlighted), Protocols, RSA Keys, Statistics, and Advanced. The main panel is titled 'Name Resolution' and contains several checkboxes: 'Resolve MAC addresses' (checked), 'Resolve transport names' (unchecked), 'Resolve network (IP) addresses' (unchecked), 'Use captured DNS packet data for address resolution' (checked), 'Use an external network name resolver' (checked), and 'Use custom list of DNS servers for name resolution' (unchecked). Below these are fields for 'DNS Servers' with an 'Edit...' button, 'Maximum concurrent requests' set to 500, and several other unchecked options: 'Only use the profile "hosts" file', 'Resolve VLAN IDs' (highlighted in light blue), 'Resolve SS7 PCs', 'Enable OID resolution', and 'Suppress SMI errors'. At the bottom, there are three more 'Edit...' buttons for 'SMI (MIB and PIB) paths', 'SMI (MIB and PIB) modules', and 'MaxMind database directories'.





# example



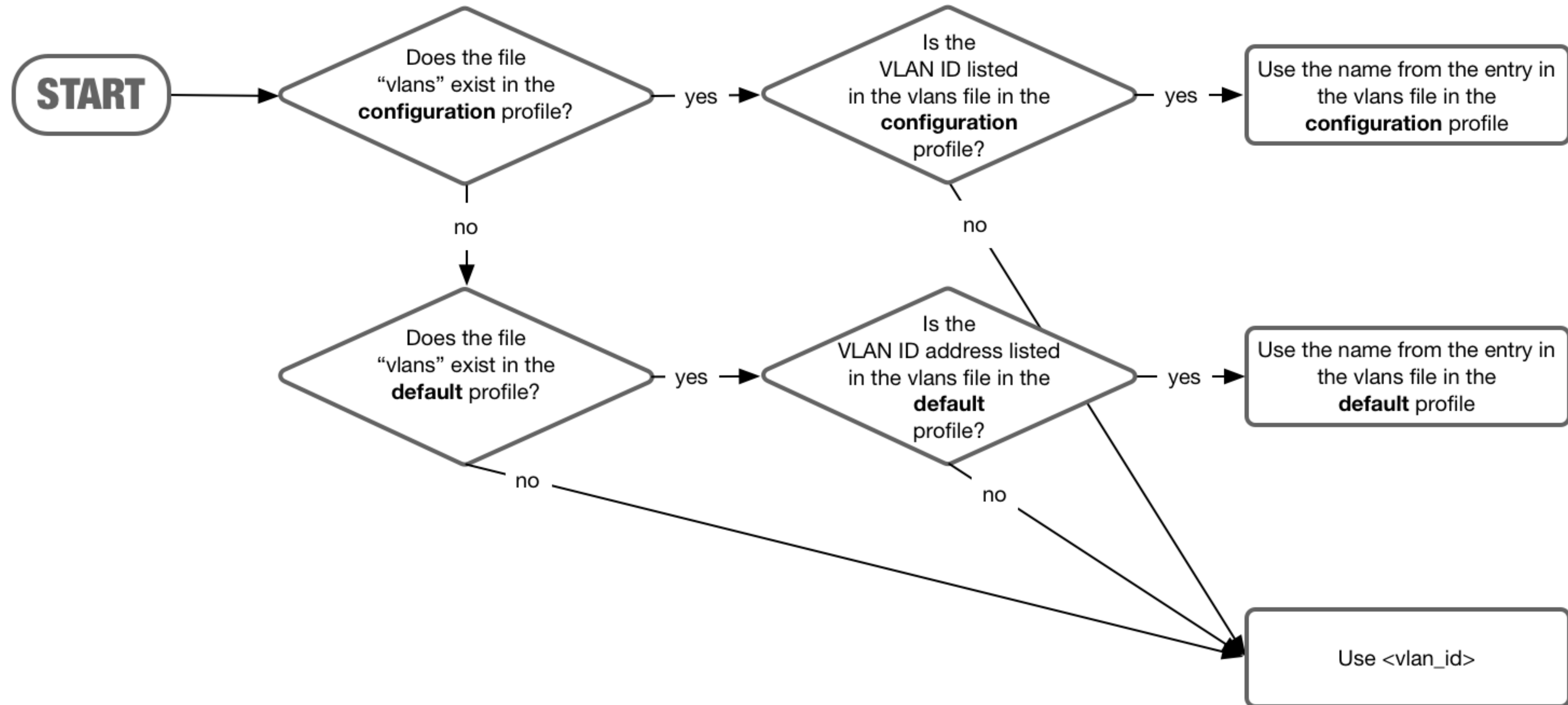
```
sake — -bash — 66x6
[sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/vlans
1102 PROFILE_1102
[sake@MacSake:~$ cat .config/wireshark/vlans
1102 DEFAULT_1102
1112 DEFAULT_1112
sake@MacSake:~$
```

vlan.id						
No.	Time	VLAN	Name	HW-src	HW-dst	
7	14.001044496	1102	PROFILE_1102	SYSTEM_PBX	Broadcast	
8	15.002258560	1102	PROFILE_1102	SYSTEM_PBX	Broadcast	
9	16.004277768	1102	PROFILE_1102	SYSTEM_PBX	Broadcast	
10	18.001607320	1102	PROFILE_1102	SYSTEM_PBX	Broadcast	
11	19.004231408	1102	PROFILE_1102	SYSTEM_PBX	Broadcast	
12	20.006233496	1102	PROFILE_1102	SYSTEM_PBX	Broadcast	
13	21.130382248	1112	<1112>	x201.local	Broadcast	
				rtr-lan-tel.ut...	x201.local	
				x201.local	Broadcast	
				rtr-lan-tel.ut...	x201.local	
				x201.local	rtr-lan-tel.ut	
				rtr-lan-tel.ut...	x201.local	

```
▶ Frame 12: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, id 0
▶ Ethernet II, Src: SYSTEM_PBX (00:0c:29:19:74:6f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1102
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  .... 0100 0100 1110 = ID: 1102
  [Name: PROFILE_1102]
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
  Trailer: 000000009ee45bb1
▶ Address Resolution Protocol (request)
```



# VLAN Resolution Process







# Transport name resolution



- disabled by default
- "services" files
  - gives individual VLAN ID's a name
  - manually edited
    - ▶ located in configuration profile
    - ▶ located in default profile
    - ▶ located in global configuration
- **NOTE: services files seem to only be loaded at Wireshark startup, not when profiles are switched (bug?)**

```

▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)

```

The image shows the 'Name Resolution' settings dialog box in Wireshark. The 'Name Resolution' tab is selected in the left sidebar. The 'Resolve transport names' checkbox is unchecked and highlighted in pink. Other settings include 'Resolve MAC addresses' (checked), 'Resolve network (IP) addresses' (unchecked), 'Use captured DNS packet data for address resolution' (checked), 'Use an external network name resolver' (checked), and 'Use custom list of DNS servers for name resolution' (unchecked). There are also fields for 'DNS Servers', 'Maximum concurrent requests' (set to 500), and several 'Edit...' buttons for SMI paths and modules.



# example



```
sake — -bash — 66x5
[sake@MacSake:~]$ cat .config/wireshark/profiles/SF21VUS/services
profile1024 1024/udp
[sake@MacSake:~]$ cat .config/wireshark/services
cat: .config/wireshark/services: No such file or directory
[sake@MacSake:~]$
```

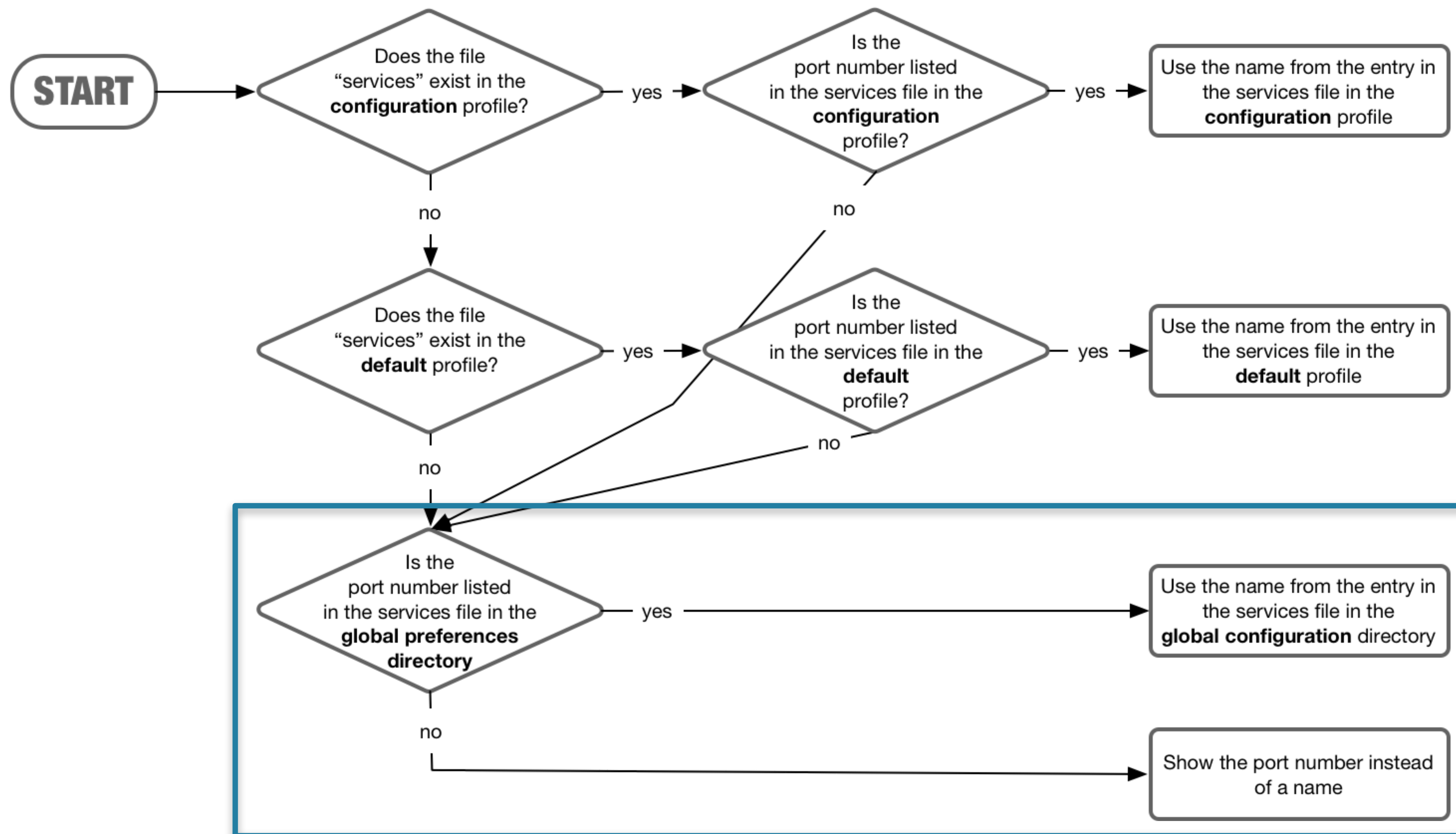
x201.local	ns.SYN-bit...	37301	domain	DNS
ns.SYN-bit.voip	x201.local	domain	37301	DNS
10.0.102.103	ns.SYN-bit...	profile1024	domain	DNS
ns.SYN-bit.voip	10.0.102.103	domain	profil...	DNS
10.0.102.103	ns.SYN-bit...	blackjack	domain	DNS
ns.SYN-bit.voip	10.0.102.103	domain	blackj...	DNS
10.0.102.103	ns.SYN-bit...	cap	domain	DNS
		domain	cap	DNS
		1028	domain	DNS
		domain	1028	DNS

```
▶ Frame 131: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface unknown, id 0
▶ Ethernet II, Src: Avaya_57:17:88 (00:1b:4f:57:17:88), Dst: rtr-lan-tel.ams.SYN-bit.voip (00:0c:29:14:1b:85)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1102
▶ Internet Protocol Version 4, Src: 10.0.102.103 (10.0.102.103), Dst: ns.SYN-bit.voip (10.0.103.1)
▼ User Datagram Protocol, Src Port: profile1024 (1024), Dst Port: domain (53)
  Source Port: profile1024 (1024)
  Destination Port: domain (53)
  Length: 42
  Checksum: 0xd7b8 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 20]
  ▶ [Timestamps]
  UDP payload (34 bytes)
▶ Domain Name System (query)
```





# Transport Resolution Process





# MAC address resolution



- enabled by default
- Sources:
  - "ethers" files
    - ▶ gives individual mac addresses a name
    - ▶ manually edited
      - located in configuration profile
      - located in default profile
      - located in system directory
  - "manuf" file
    - ▶ handles OUI lookups and other groups
    - ▶ generated by wireshark compilation
      - located in global configuration directory
  - mDNS/DNS resolution in the pcap file
    - ▶ NOTE: mDNS/DNS information from packets don't seem to be flushed when opening a new file (bug?)

```

▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)

```

The image shows the 'Name Resolution' settings dialog in Wireshark. The 'Name Resolution' section is selected in the left sidebar. The following options are checked:

- Resolve MAC addresses
- Use captured DNS packet data for address resolution
- Use an external network name resolver

Other options shown but unchecked include: Resolve transport names, Resolve network (IP) addresses, and Use custom list of DNS servers for name resolution. There are also fields for 'DNS Servers', 'Maximum concurrent requests' (set to 500), and buttons for 'Edit...' for SMI (MIB and PIB) paths, modules, and MaxMind database directories.





# manuf file???



- Sources

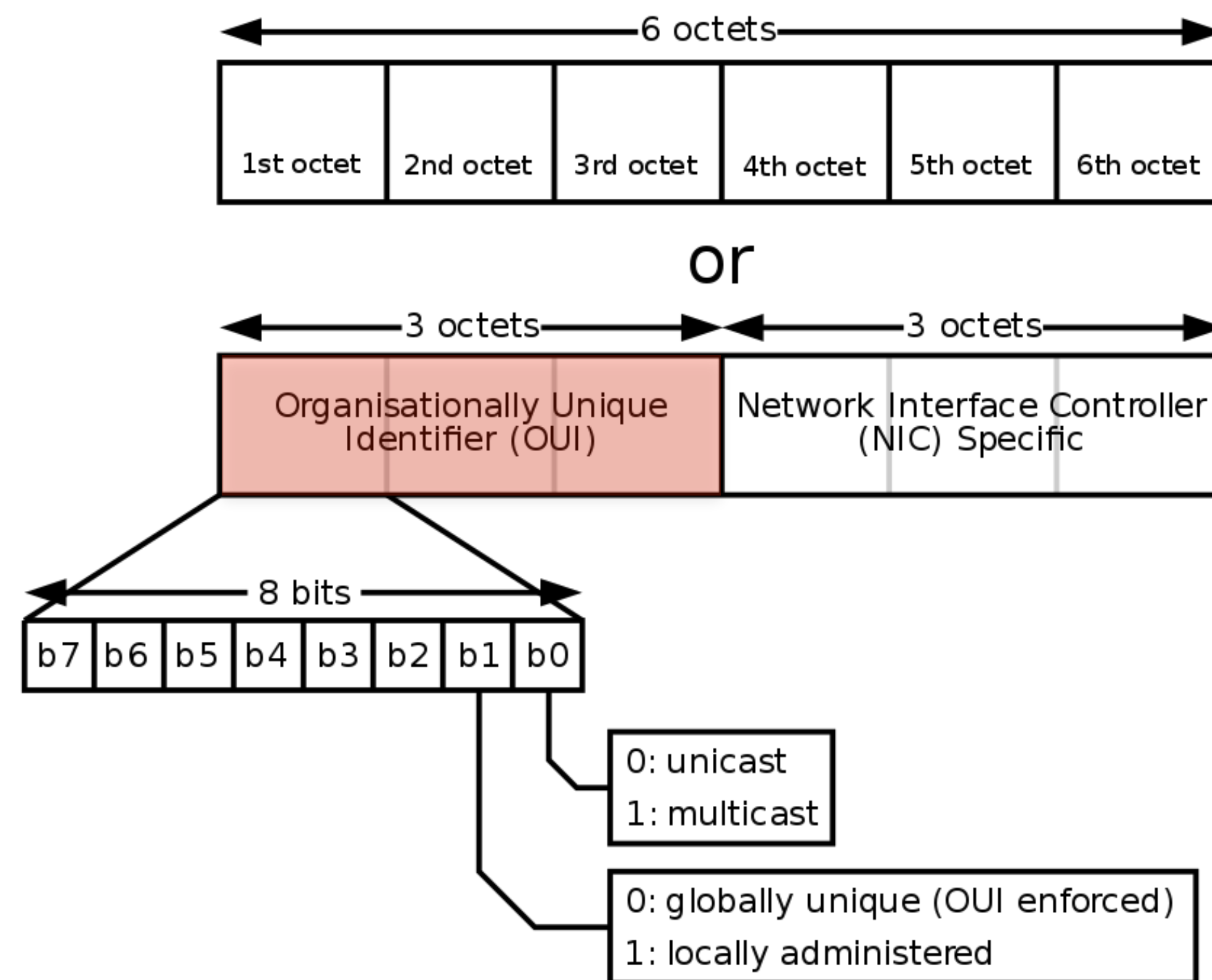
- Wireshark's own lists
- Michael Patton's "Ethernet Codes Master Page"
- The IEEE OUI listings

- Compilation

- ./tools/make-manuf.py
- with names truncated to 8 characters

- Destination

- manuf file  
(see: <https://gitlab.com/wireshark/wireshark/raw/master/manuf>)





# example



```
sake — -bash — 96x20
[sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/ethers
00:0c:29:14:1b:85 PROFILE_85
00:0c:29:19:74:6f PROFILE_6F
00:1b:4f:57:17:88 PROFILE_PHONE88
01:00:5e:00:00:fb PROFILE_MULTIKAST
ff:ff:ff:ff:ff:ff PROFILE_BROODKAST
[sake@MacSake:~$ cat .config/wireshark/ethers
00:0c:29:19:74:6f DEFAULT_6F
00:0c:29:21:88:48 DEFAULT_48
00:1b:4f:57:21:87 DEFAULT_PHONE87
01:00:5e:00:00:fb DEFAULT_MULTIKAST
ff:ff:ff:ff:ff:ff DEFAULT_BROODKAST
[sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/ethers
00:0c:29:a6:b2:5d GLOBAL_5D
[sake@MacSake:~$ cat /etc/ethers
00:1b:4f:57:21:87 SYSTEM_PHONE87
00:1b:4f:57:17:88 SYSTEM_PHONE88
01:00:5e:00:00:fb SYSTEM_MULTIKAST
ff:ff:ff:ff:ff:ff SYSTEM_BROODKAST
sake@MacSake:~$
```

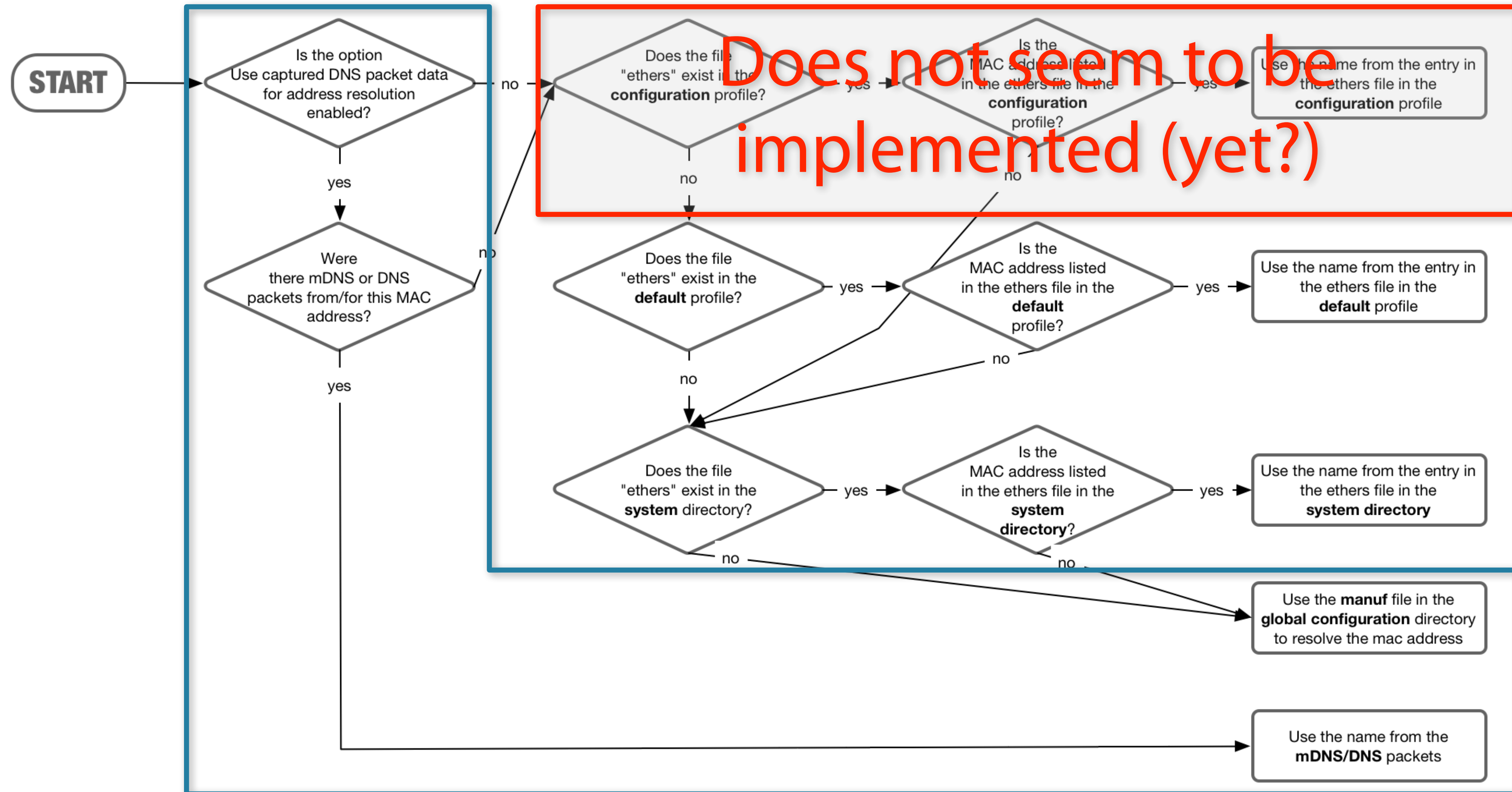
When "Use captured DNS packet data for address resolution" is enabled

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
VMware_14:1b:85	83	13k	42	10k		
pbx.SYN-bit.voip	65	21k	46	17k		
DEFAULT_48	105	23k	52	18k		
pbx.rtd.SYN-bit.voip	14	6969	7	2935		
VMware_b0:c9:1c	1.420	193k	743	87k		
VMware_e1:06:96	9	840	5	454		
SYSTEM_PHONE88	138	37k	69	11k		
DEFAULT_PHONE87	127	33k	68	11k		
DEFAULT_MULTIKAST	13	2141	0	0		
x201.local	1.445	197k	697	109k		
Broadcast	39	6834	0	0		





# MAC Resolution Process





# Network Address Resolution



- disabled by default
- many sources:
  - Captured forward DNS lookups (A/AAAA records)
  - Edit Resolved Name (rightclick option)
    - ▶ You will be asked if you want to save the changes!
  - PCAPNG Name Resolution Block(s) (NRB)
  - "hosts" files in multiple locations
    - ▶ Use all locations or just in the configuration profile
  - Explicit reverse DNS lookups (PTR records)
    - ▶ optional: use specific servers
- **NOTE:** Reloading a file or changing settings does not always fully remove the name resolution cache

```
▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)
```

The image shows the 'Name Resolution' settings panel in Wireshark. The 'Name Resolution' section is highlighted in blue in the left sidebar. The main panel has a green background and contains the following settings:

- Resolve MAC addresses
- Resolve transport names
- Resolve network (IP) addresses
- Use captured DNS packet data for address resolution
- Use an external network name resolver
- Use custom list of DNS servers for name resolution

DNS Servers: Edit...

Maximum concurrent requests: 500

- Only use the profile "hosts" file
- Resolve VLAN IDs
- Resolve SS7 PCs
- Enable OID resolution
- Suppress SMI errors

SMI (MIB and PIB) paths: Edit...

SMI (MIB and PIB) modules: Edit...

MaxMind database directories: Edit...





# example - hosts



```
sake -- -bash -- 96x17
sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/hosts
10.0.102.103 PROFILE_PHONE102
10.0.102.254 PROFILE_GW102
10.0.112.254 PROFILE_GW112
10.0.122.1 PROFILE_PBX122
sake@MacSake:~$ cat .config/wireshark/hosts
10.0.112.1 DEFAULT_PBX112
10.0.112.254 DEFAULT_GW112
10.0.122.254 DEFAULT_GW122
sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/share/wireshark/hosts
10.0.102.254 GLOBAL_GW102
10.0.122.254 GLOBAL_GW122
sake@MacSake:~$ grep SYSTEM /etc/hosts
10.0.102.1 SYSTEM_PBX
10.0.103.1 SYSTEM_DNS
13.225.234.215 SYSTEM_NEVERSSL
sake@MacSake:~$
```

Resolve network (IP) addresses  
 Use captured DNS packet data for address resolution  
 Use an external network name resolver  
 Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

frame.number in {14 83 109 131..133 145 584 259 488 491 517}

No.	Time	VLAN	Source-IP	Source	Destination	Destination-IP	Protocol
14	21.135129736	1112	10.0.112.254	PROFILE_GW112	10.0.112.103	10.0.112.103	DHCP
83	39.189200608	1102	10.0.102.254	PROFILE_GW102	PROFILE_PHONE102	10.0.102.103	ICMP
109	46.036142032	1122	10.0.122.254	GLOBAL_GW122	10.0.122.102	10.0.122.102	ICMP
131	50.318554736	1102	10.0.102.103	PROFILE_PHONE102	10.0.103.1	10.0.103.1	DNS
132	50.319152872	1102	10.0.103.1	10.0.103.1	PROFILE_PHONE102	10.0.102.103	DNS
133	50.320429696	1102	10.0.102.103	PROFILE_PHONE102	10.0.102.1	10.0.102.1	TCP
145	50.361301552	1102	10.0.102.103	PROFILE_PHONE102	10.0.103.1	10.0.103.1	DNS
259	57.985889800	1122	10.0.122.1	PROFILE_PBX122	10.0.122.102	10.0.122.102	SIP
488	95.365501768	1112	10.0.112.103	10.0.112.103	10.0.103.1	10.0.103.1	DNS
491	95.403560792	1112	10.0.103.1	10.0.103.1	10.0.112.103	10.0.112.103	DNS
517	96.481756384	1112	10.0.112.103	10.0.112.103	13.225.234.215	13.225.234.215	TCP
584	101.665985656	1112	10.0.112.103	10.0.112.103	10.0.112.1	10.0.112.1	ICMP





# example - hosts



```
sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/hosts
10.0.102.103 PROFILE_PHONE102
10.0.102.254 PROFILE_GW102
10.0.112.254 PROFILE_GW112
10.0.122.1 PROFILE_PBX122
sake@MacSake:~$ cat .config/wireshark/hosts
10.0.112.1 DEFAULT_PBX112
10.0.112.254 DEFAULT_GW112
10.0.122.254 DEFAULT_GW122
sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/share/wireshark/hosts
10.0.102.254 GLOBAL_GW102
10.0.122.254 GLOBAL_GW122
sake@MacSake:~$ grep SYSTEM /etc/hosts
10.0.102.1 SYSTEM_PBX
10.0.103.1 SYSTEM_DNS
13.225.234.215 SYSTEM_NEVERSSL
sake@MacSake:~$
```

Resolve network (IP) addresses  
 Use captured DNS packet data for address resolution  
 Use an external network name resolver  
 Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

frame.number in {14 83 109 131..133 145 584 259 488 491 517}

No.	Time	VLAN	Source-IP	Source	Destination	Destination-IP	Protocol
14	21.135129736	1112	10.0.112.254	PROFILE_GW112	10.0.112.103	10.0.112.103	DHCP
83	39.189200608	1102	10.0.102.254	PROFILE_GW102	PROFILE_PHONE102	10.0.102.103	ICMP
109	46.036142032	1122	10.0.122.254	GLOBAL_GW122	10.0.122.102	10.0.122.102	ICMP
131	50.318554736	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_DNS	10.0.103.1	DNS
132	50.319152872	1102	10.0.103.1	SYSTEM_DNS	PROFILE_PHONE102	10.0.102.103	DNS
133	50.320429696	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_PBX	10.0.102.1	TCP
145	50.361301552	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_DNS	10.0.103.1	DNS
259	57.985889800	1122	10.0.122.1	PROFILE_PBX122	10.0.122.102	10.0.122.102	SIP
488	95.365501768	1112	10.0.112.103	10.0.112.103	SYSTEM_DNS	10.0.103.1	DNS
491	95.403560792	1112	10.0.103.1	SYSTEM_DNS	10.0.112.103	10.0.112.103	DNS
517	96.481756384	1112	10.0.112.103	10.0.112.103	SYSTEM_NEVERSSL	13.225.234.215	TCP
584	101.665985656	1112	10.0.112.103	10.0.112.103	10.0.112.1	10.0.112.1	ICMP





# example - hosts



```
sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/hosts
10.0.102.103 PROFILE_PHONE102
10.0.102.254 PROFILE_GW102
10.0.112.254 PROFILE_GW112
10.0.122.1 PROFILE_PBX122
sake@MacSake:~$ cat .config/wireshark/hosts
10.0.112.1 DEFAULT_PBX112
10.0.112.254 DEFAULT_GW112
10.0.122.254 DEFAULT_GW122
sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/share/wireshark/hosts
10.0.102.254 GLOBAL_GW102
10.0.122.254 GLOBAL_GW122
sake@MacSake:~$ grep SYSTEM /etc/hosts
10.0.102.1 SYSTEM_PBX
10.0.103.1 SYSTEM_DNS
13.225.234.215 SYSTEM_NEVERSSL
sake@MacSake:~$
```

Resolve network (IP) addresses  
 Use captured DNS packet data for address resolution  
 Use an external network name resolver  
 Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

frame.number in {14 83 109 131..133 145 584 259 488 491 517}

No.	Time	VLAN	Source-IP	Source	Destination	Destination-IP	Protocol
14	21.135129736	1112	10.0.112.254	PROFILE_GW112	10.0.112.103	10.0.112.103	DHCP
83	39.189200608	1102	10.0.102.254	PROFILE_GW102	PROFILE_PHONE102	10.0.102.103	ICMP
109	46.036142032	1122	10.0.122.254	10.0.122.254	10.0.122.102	10.0.122.102	ICMP
131	50.318554736	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_DNS	10.0.103.1	DNS
132	50.319152872	1102	10.0.103.1	SYSTEM_DNS	PROFILE_PHONE102	10.0.102.103	DNS
133	50.320429696	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_PBX	10.0.102.1	TCP
145	50.361301552	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_DNS	10.0.103.1	DNS
259	57.985889800	1122	10.0.122.1	PROFILE_PBX122	10.0.122.102	10.0.122.102	SIP
488	95.365501768	1112	10.0.112.103	10.0.112.103	SYSTEM_DNS	10.0.103.1	DNS
491	95.403560792	1112	10.0.103.1	SYSTEM_DNS	10.0.112.103	10.0.112.103	DNS
517	96.481756384	1112	10.0.112.103	10.0.112.103	SYSTEM_NEVERSSL	13.225.234.215	TCP
584	101.665985656	1112	10.0.112.103	10.0.112.103	10.0.112.1	10.0.112.1	ICMP





# example - hosts



```
sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/hosts
cat: .config/wireshark/profiles/SF21VUS/hosts: No such file or directory
sake@MacSake:~$ cat .config/wireshark/hosts
10.0.112.1    DEFAULT_PBX112
10.0.112.254  DEFAULT_GW112
10.0.122.254  DEFAULT_GW122
sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/share/wireshark/hosts
10.0.102.254  GLOBAL_GW102
10.0.122.254  GLOBAL_GW122
sake@MacSake:~$ grep SYSTEM /etc/hosts
10.0.102.1    SYSTEM_PBX
10.0.103.1    SYSTEM_DNS
13.225.234.215 SYSTEM_NEVERSSL
sake@MacSake:~$
```

Resolve network (IP) addresses  
 Use captured DNS packet data for address resolution  
 Use an external network name resolver  
 Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

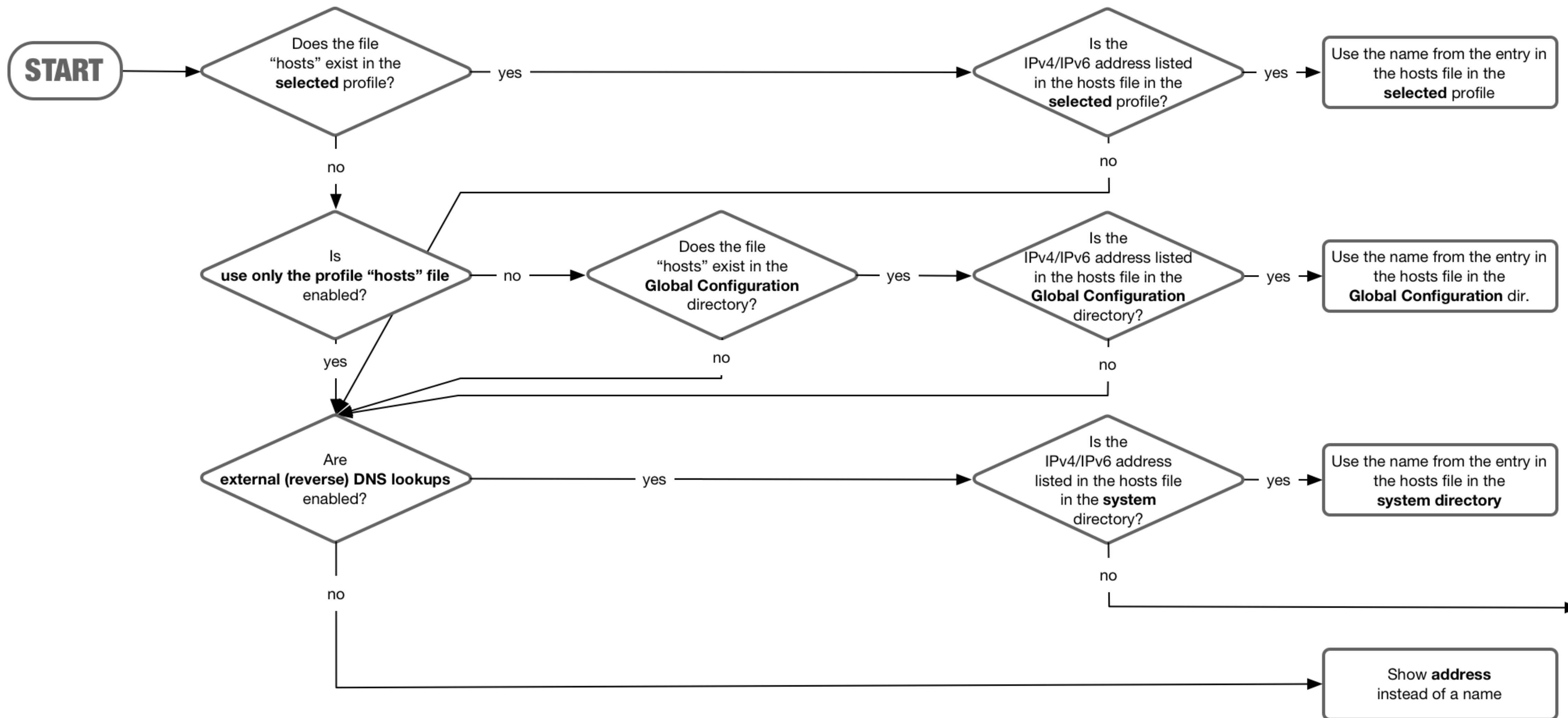
frame.number in {14 83 109 131..133 145 584 259 488 491 517}

No.	Time	VLAN	Source-IP	Source	Destination	Destination-IP	Protocol
14	21.135129736	1112	10.0.112.254	10.0.112.254	10.0.112.103	10.0.112.103	DHCP
83	39.189200608	1102	10.0.102.254	GLOBAL_GW102	10.0.102.103	10.0.102.103	ICMP
109	46.036142032	1122	10.0.122.254	GLOBAL_GW122	10.0.122.102	10.0.122.102	ICMP
131	50.318554736	1102	10.0.102.103	10.0.102.103	SYSTEM_DNS	10.0.103.1	DNS
132	50.319152872	1102	10.0.103.1	SYSTEM_DNS	10.0.102.103	10.0.102.103	DNS
133	50.320429696	1102	10.0.102.103	10.0.102.103	SYSTEM_PBX	10.0.102.1	TCP
145	50.361301552	1102	10.0.102.103	10.0.102.103	SYSTEM_DNS	10.0.103.1	DNS
259	57.985889800	1122	10.0.122.1	10.0.122.1	10.0.122.102	10.0.122.102	SIP
488	95.365501768	1112	10.0.112.103	10.0.112.103	SYSTEM_DNS	10.0.103.1	DNS
491	95.403560792	1112	10.0.103.1	SYSTEM_DNS	10.0.112.103	10.0.112.103	DNS
517	96.481756384	1112	10.0.112.103	10.0.112.103	SYSTEM_NEVERSSL	13.225.234.215	TCP
584	101.665985656	1112	10.0.112.103	10.0.112.103	10.0.112.1	10.0.112.1	ICMP





# hosts files!





# example - external resolver



```
sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/hosts
10.0.102.103 PROFILE_PHONE102
10.0.102.254 PROFILE_GW102
10.0.112.254 PROFILE_GW112
10.0.122.1 PROFILE_PBX122
sake@MacSake:~$ cat .config/wireshark/hosts
10.0.112.1 DEFAULT_PBX112
10.0.112.254 DEFAULT_GW112
10.0.122.254 DEFAULT_GW122
sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/share/wireshark/hosts
10.0.102.254 GLOBAL_GW102
10.0.122.254 GLOBAL_GW122
sake@MacSake:~$ grep SYSTEM /etc/hosts
10.0.102.1 SYSTEM_PBX
13.225.234.215 SYSTEM_NEVERSSL
sake@MacSake:~$
```

Resolve network (IP) addresses  
 Use captured DNS packet data for address resolution  
 Use an external network name resolver  
 Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent  
 Only use the p...

DNS Servers

IP address  
10.0.103.1

+ - [up] [down] [search] /Users/sak...ns\_servers

Help Copy from Cancel OK

(sip.Method== REGISTER || dns.id in {0x00000007 0xd72c}) || (ip.addr==13.0.0.0/8 && tcp.connection.syn)

No.	Time	VLAN	Source-IP	Source	Destination	Destination-IP	Protocol
170	51.076826064	1102	10.0.102.103	PROFILE_PHONE102	voip-services.SYN-bit.voip	10.0.103.1	DNS
171	51.077077808	1102	10.0.103.1	voip-services.SYN-bit...	PROFILE_PHONE102	10.0.102.103	DNS
172	51.106324392	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_PBX	10.0.102.1	SIP
174	51.115816848	1102	10.0.102.103	PROFILE_PHONE102	SYSTEM_PBX	10.0.102.1	SIP
245	57.875214536	1122	10.0.122.102	10.0.122.102	voip-services.SYN-bit.voip	10.0.103.1	DNS
246	57.896070264	1122	10.0.103.1	voip-services.SYN-bit...	10.0.122.102	10.0.122.102	DNS
249	57.924321448	1122	10.0.122.102	10.0.122.102	PROFILE_PBX122	10.0.122.1	SIP
251	57.941561656	1122	10.0.122.102	10.0.122.102	PROFILE_PBX122	10.0.122.1	SIP
488	95.365501768	1112	10.0.112.103	10.0.112.103	voip-services.SYN-bit.voip	10.0.103.1	DNS
491	95.403560792	1112	10.0.103.1	voip-services.SYN-bit...	10.0.112.103	10.0.112.103	DNS
492	95.404465224	1112	10.0.112.103	10.0.112.103	server-13-225-234-89.bru5...	13.225.234.89	TCP
517	96.481756384	1112	10.0.112.103	10.0.112.103	SYSTEM_NEVERSSL	13.225.234.215	TCP
553	97.595500592	1112	10.0.112.103	10.0.112.103	SYSTEM_NEVERSSL	13.225.234.215	TCP





# example - use DNS packets



```
sake@MacSake:~$ cat .config/wireshark/profiles/SF21VUS/hosts
10.0.102.103 PROFILE_PHONE102
10.0.102.254 PROFILE_GW102
10.0.112.254 PROFILE_GW112
10.0.122.1 PROFILE_PBX122
sake@MacSake:~$ cat .config/wireshark/hosts
10.0.112.1 DEFAULT_PBX112
10.0.112.254 DEFAULT_GW112
10.0.122.254 DEFAULT_GW122
sake@MacSake:~$ cat /Applications/Wireshark-3.4.8.app/Contents/Resources/share/wireshark/hosts
10.0.102.254 GLOBAL_GW102
10.0.122.254 GLOBAL_GW122
sake@MacSake:~$ grep SYSTEM /etc/hosts
10.0.102.1 SYSTEM_PBX
13.225.234.215 SYSTEM_NEVERSSL
sake@MacSake:~$
```

Resolve network (IP) addresses  
 Use captured DNS packet data for address resolution  
 Use an external network name resolver  
 Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

(sip.Method== REGISTER || dns.id in {0x00000007 0xd72c}) || (ip.addr==13.0.0.0/8 && tcp.connection.syn)

No.	Time	Source-IP	Source	Destination	Destination-IP	Info
170	51.076826064	10.0.102.103	PROFILE_PHONE102	voip-services.SYN-bit.voip	10.0.103.1	Standard query 0x0007 A pbx.syn-bit.voip
171	51.077077808	10.0.103.1	voip-services.SYN-bit...	PROFILE_PHONE102	10.0.102.103	Standard query response 0x0007 A pbx.syn-bit.voip A 10.0.102.1 NS ns.SYN-bit.voip A 10.0.103.1
172	51.106324392	10.0.102.103	PROFILE_PHONE102	SYSTEM_PBX	10.0.102.1	Request: REGISTER sip:pbx.syn-bit.voip (1 binding)
174	51.115816848	10.0.102.103	PROFILE_PHONE102	SYSTEM_PBX	10.0.102.1	Request: REGISTER sip:pbx.syn-bit.voip (1 binding)
245	57.875214536	10.0.122.102	10.0.122.102	voip-services.SYN-bit.voip	10.0.103.1	Standard query 0x0007 A pbx.rtd.syn-bit.voip
246	57.896070264	10.0.103.1	voip-services.SYN-bit...	10.0.122.102	10.0.122.102	Standard query response 0x0007 A pbx.rtd.syn-bit.voip A 10.0.122.1 NS ns.SYN-bit.voip A 10.0.103.1
249	57.924321448	10.0.122.102	10.0.122.102	pbx.rtd.SYN-bit.voip	10.0.122.1	Request: REGISTER sip:pbx.rtd.syn-bit.voip (1 binding)
251	57.941561656	10.0.122.102	10.0.122.102	pbx.rtd.SYN-bit.voip	10.0.122.1	Request: REGISTER sip:pbx.rtd.syn-bit.voip (1 binding)
488	95.365501768	10.0.112.103	x201.local	voip-services.SYN-bit.voip	10.0.103.1	Standard query 0xd72c A neverssl.com OPT
491	95.403560792	10.0.103.1	voip-services.SYN-bit...	x201.local	10.0.112.103	Standard query response 0xd72c A neverssl.com A 13.225.234.89 A 13.225.234.210 A 13.225.234.27 A 13.225.234.215 OPT
492	95.404465224	10.0.112.103	x201.local	neverssl.com	13.225.234.89	48058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1887534643 TSecr=0 WS=128
517	96.481756384	10.0.112.103	x201.local	neverssl.com	13.225.234.215	39374 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=145010618 TSecr=0 WS=128
553	97.595500592	10.0.112.103	x201.local	neverssl.com	13.225.234.215	1337 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=145011731 TSecr=0 WS=128





# example - Name Resolution Blocks



▼ Block: Name Resolution Block  
 ▶ Block Type: Name Resolution Block (0x00000004)  
 Block Length: 80  
 ▼ Block Data  
 ▼ Records  
 ▼ Record: IPv4 Record = SYSTEM\_PBX  
 Code: IPv4 Record (1)  
 Length: 12  
 IPv4: SYSTEM\_PBX (10.0.102.1)  
 Name: NRB\_PBX  
 ▼ Record: IPv4 Record = PROFILE\_PHONE102  
 Code: IPv4 Record (1)  
 Length: 17  
 IPv4: PROFILE\_PHONE102 (10.0.102.103)  
 Name: NRB\_PHONE103  
 Record Padding  
 ▼ Record: IPv4 Record = server-13-225-234-89.bru50.r.cloudfront.net  
 Code: IPv4 Record (1)  
 Length: 17  
 IPv4: server-13-225-234-89.bru50.r.cloudfront.net (13.225.234.89)  
 Name: NRB\_NEVERSSL  
 Record Padding  
 ▶ Record: End of Records

- Resolve network (IP) addresses
- Use captured DNS packet data for address resolution
- Use an external network name resolver
- Use custom list of DNS servers for name resolution

DNS Servers

Maximum concurrent requests

Only use the profile "hosts" file

0007 0xd72c) || (ip.addr==13.0.0.0/8 && tcp.connection.syn)

Offset	Source IP	Source	Destination	Destination-IP	Protocol
170	51.070620004	1102 10.0.102.103	NRB_PHONE103	voip-services.SYN-bit.voip	10.0.103.1 DNS
171	51.077077808	1102 10.0.103.1	voip-services.SYN-bit...	NRB_PHONE103	10.0.102.103 DNS
172	51.106324392	1102 10.0.102.103	NRB_PHONE103	SYSTEM_PBX	10.0.102.1 SIP
174	51.115816848	1102 10.0.102.103	NRB_PHONE103	SYSTEM_PBX	10.0.102.1 SIP
245	57.875214536	1122 10.0.122.102	10.0.122.102	voip-services.SYN-bit.voip	10.0.103.1 DNS
246	57.896070264	1122 10.0.103.1	voip-services.SYN-bit...	10.0.122.102	10.0.122.102 DNS
249	57.924321448	1122 10.0.122.102	10.0.122.102	pbx.rtd.SYN-bit.voip	10.0.122.1 SIP
251	57.941561656	1122 10.0.122.102	10.0.122.102	pbx.rtd.SYN-bit.voip	10.0.122.1 SIP
488	95.365501768	1112 10.0.112.103	x201.local	voip-services.SYN-bit.voip	10.0.103.1 DNS
491	95.403560792	1112 10.0.103.1	voip-services.SYN-bit...	x201.local	10.0.112.103 DNS
492	95.404465224	1112 10.0.112.103	x201.local	NRB_NEVERSSL	13.225.234.89 TCP
517	96.481756384	1112 10.0.112.103	x201.local	neverssl.com	13.225.234.215 TCP
553	97.595500592	1112 10.0.112.103	x201.local	neverssl.com	13.225.234.215 TCP

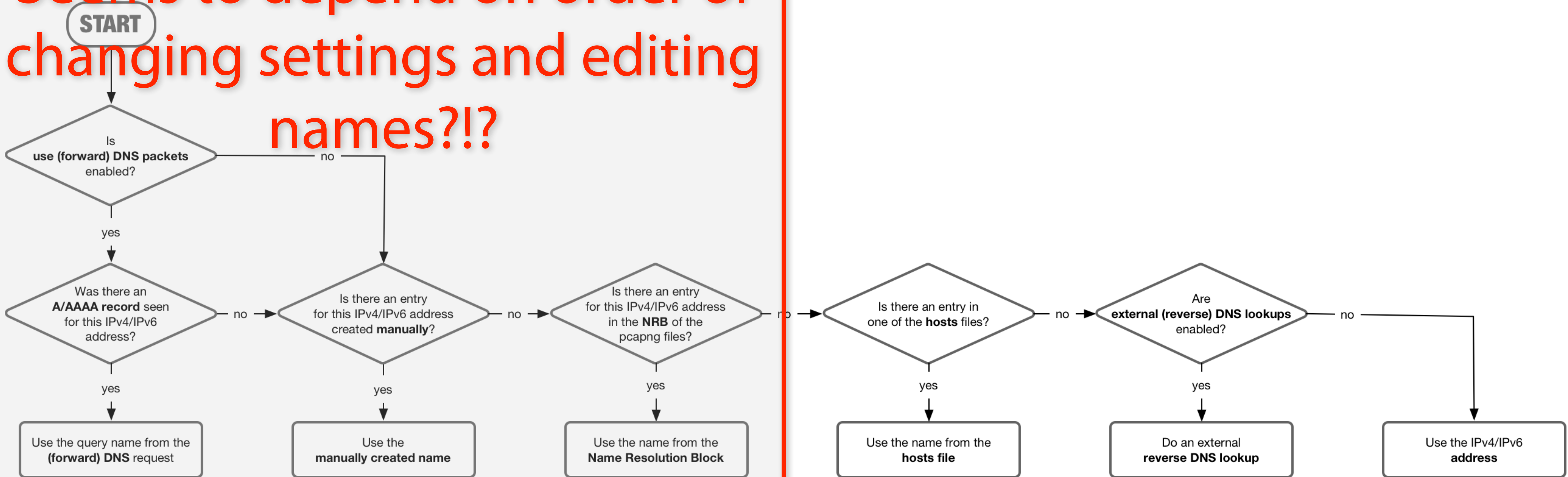




# Network Resolution Process



Seems to depend on order of changing settings and editing names?!?





# Some notes



- The order of enabling/disabling name resolution settings and editing resolved names change how things are resolved!?!
- "Save as ..." will save newly discovered hostnames into the PCAPNG file
- Some name resolving cache entries do not get cleared until you restart Wireshark
- disabling "Use DNS packets..." does not unlearn the learned name/addresses







# Adding GeoIP information



- Wireshark can use GeoLite2 databases
  - <https://dev.maxmind.com/geoip/geolite2-free-geolocation-data?lang=en>
- Database directories are profile independent
- GeoIP enhancement can be enabled per profile
- Default locations are hardcoded in Wireshark
- Possible to create your own MMDB files:
  - <https://blog.maxmind.com/2015/09/29/building-your-own-mmdb-database-for-fun-and-profit/>

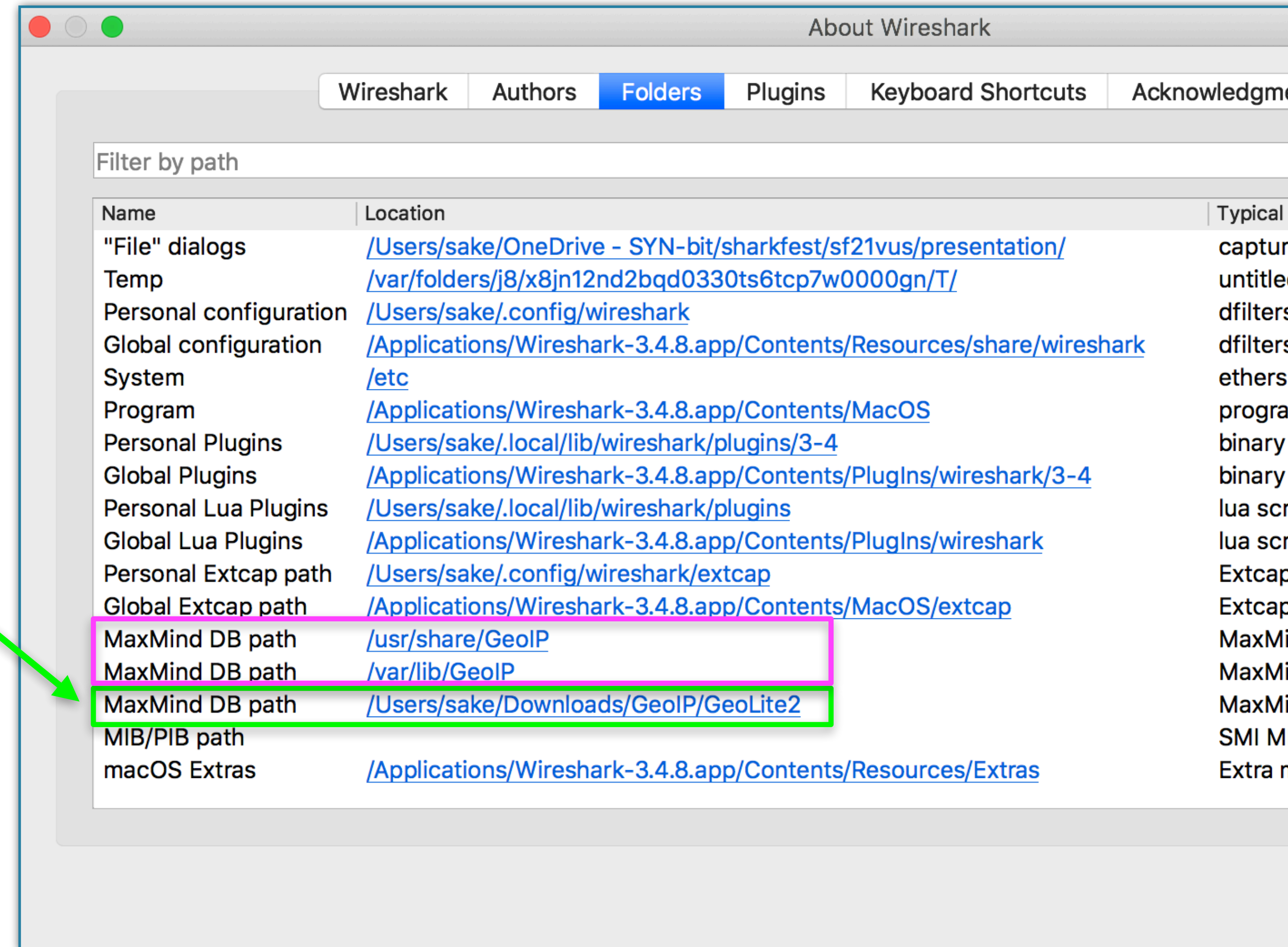
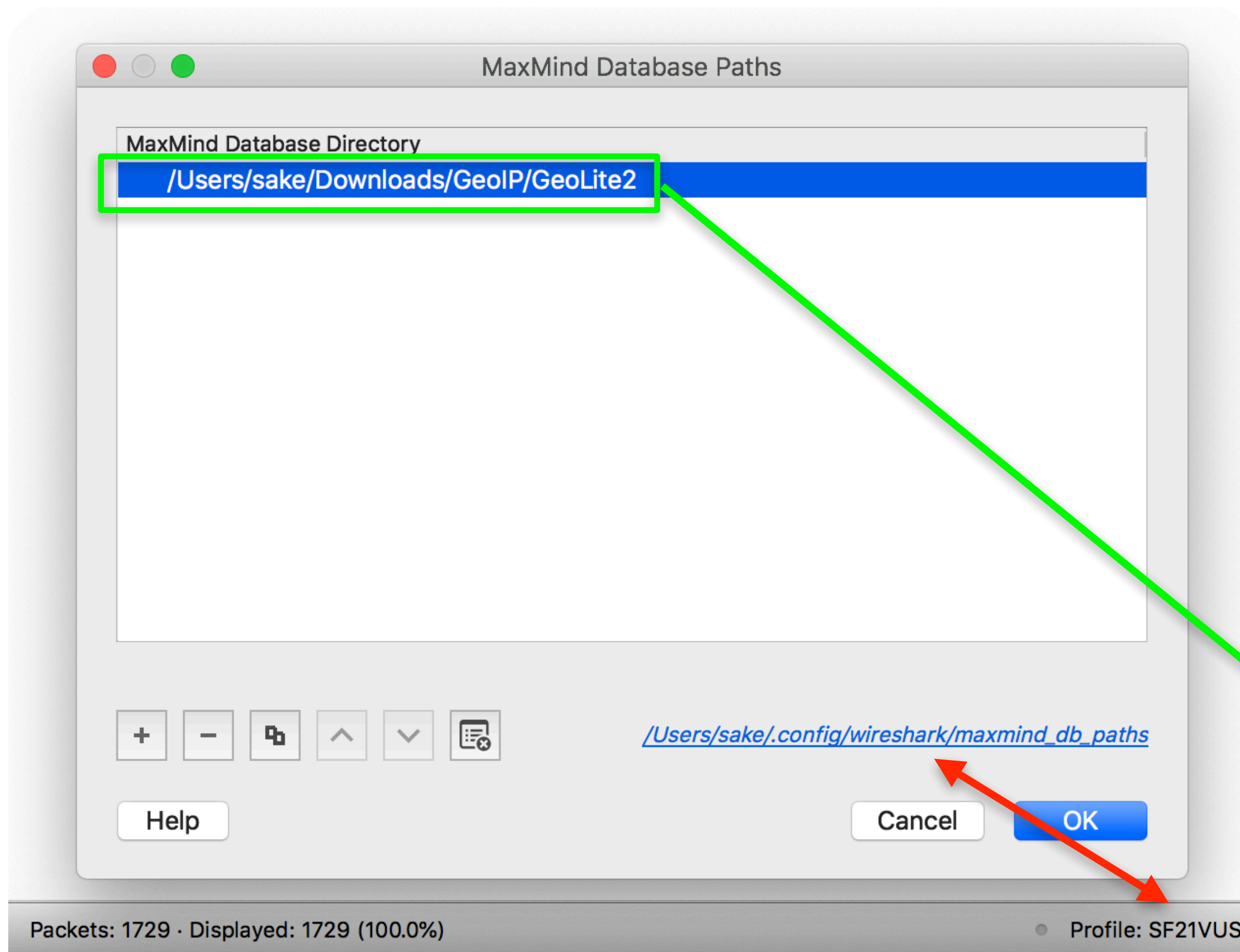
```
▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)
```

The image shows the Name Resolution settings panel in Wireshark. The left sidebar has 'Name Resolution' selected. The main panel has the following settings:

- Name Resolution**
  - Resolve MAC addresses
  - Resolve transport names
  - Resolve network (IP) addresses
  - Use captured DNS packet data for address resolution
  - Use an external network name resolver
  - Use custom list of DNS servers for name resolution
- DNS Servers: Edit...
- Maximum concurrent requests: 500
- Only use the profile "hosts" file
- Resolve VLAN IDs
- Resolve SS7 PCs
- Enable OID resolution
- Suppress SMI errors
- SMI (MIB and PIB) paths: Edit...
- SMI (MIB and PIB) modules: Edit...
- MaxMind database directories: Edit...



# Configuring MMDB Paths







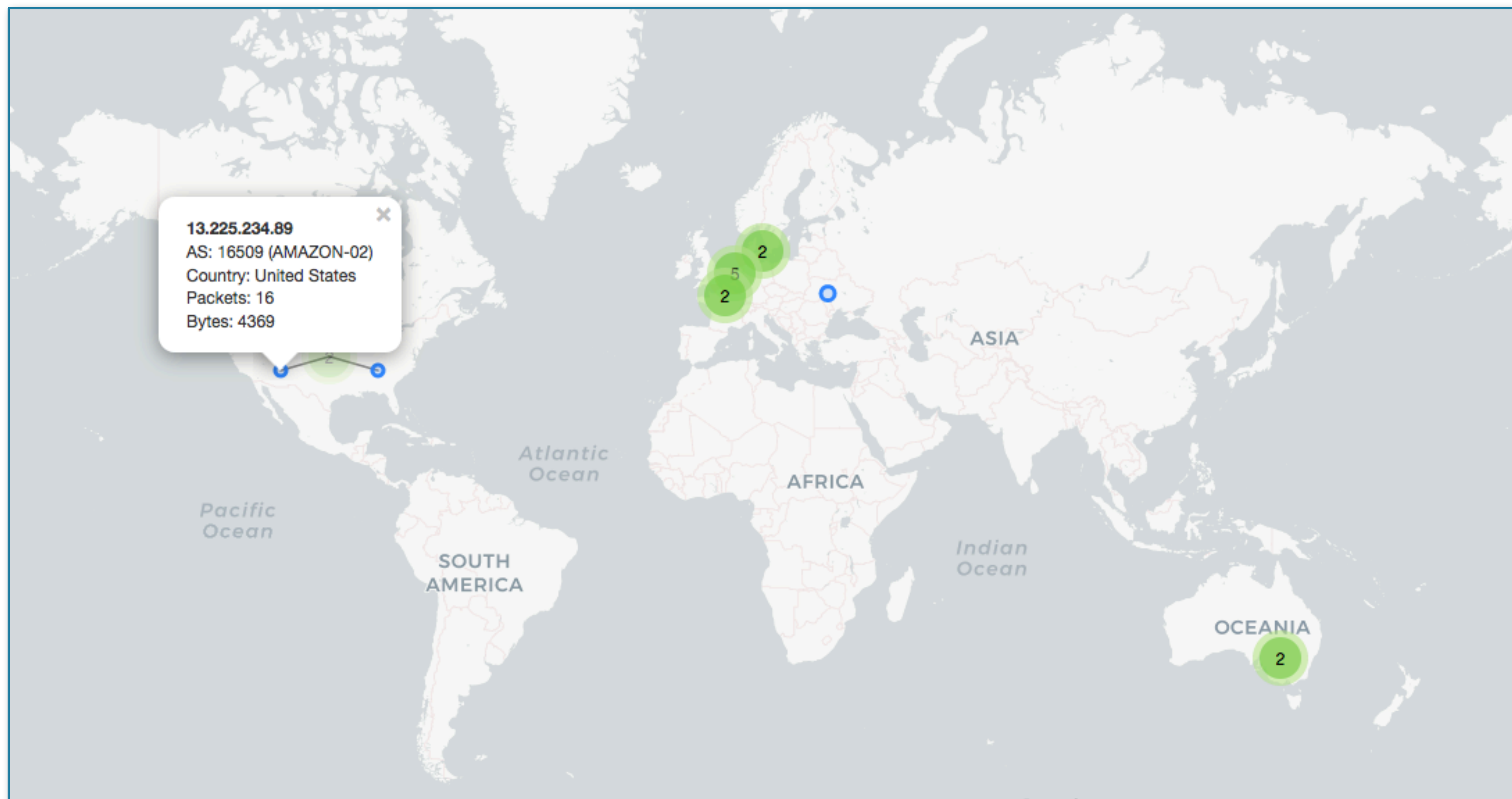
# GeoIP example



```
▶ Ethernet II, Src: x201.local (T0:0e:T1:58:72:D5), Dst: rtr-lan-tel.utr.syn-bit.voip (00:0c:29:d0:c9:1c)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▼ Internet Protocol Version 4, Src: x201.local (10.0.112.103), Dst: one.one.one.one (1.0.0.1)
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0xc85a (51290)
  ▶ Flags: 0x40, Don't fragment
  Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0xf6e6 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: x201.local (10.0.112.103)
  Destination Address: one.one.one.one (1.0.0.1)
▼ [Destination GeoIP: AU, ASN 13335, CLOUDFLARENET]
  [Destination GeoIP Country: Australia]
  [Source or Destination GeoIP Country: Australia]
  [Destination GeoIP ISO Two Letter Country Code: AU]
  [Source or Destination GeoIP ISO Two Letter Country Code: AU]
  [Destination GeoIP AS Number: 13335]
  [Source or Destination GeoIP AS Number: 13335]
  [Destination GeoIP AS Organization: CLOUDFLARENET]
  [Source or Destination GeoIP AS Organization: CLOUDFLARENET]
  [Destination GeoIP Latitude: -33.494]
  [Source or Destination GeoIP Latitude: -33.494]
  [Destination GeoIP Longitude: 143.2104]
  [Source or Destination GeoIP Longitude: 143.2104]
▶ Internet Control Message Protocol
```



# Draw a map (in endpoints)







# SNMP OID lookups



- disabled by default
- Source
  - SMI modules (MIB files)
  - Multiple paths possible
  - Paths and modules are global
    - ▶ If you change them, you need to restart Wireshark
  - Enablement is a profile setting
- Paths/module configuration is very picky

```
▶ Frame 720: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▶ Ethernet II, Src: f0:de:f1:58:72:b5, Dst: 00:0c:29:b0:c9:1c
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1112
▶ Internet Protocol Version 4, Src: 10.0.112.103, Dst: 192.168.101.1
▶ User Datagram Protocol, Src Port: 51130, Dst Port: 161
▼ Simple Network Management Protocol
  version: v2c (1)
  community: SYN-bit-public
  ▼ data: get-next-request (1)
    ▼ get-next-request
      request-id: 601920577
      error-status: noError (0)
      error-index: 0
      ▼ variable-bindings: 1 item
        ▼ 1.3.6.1.2.1.1: Value (Null)
          Object Name: 1.3.6.1.2.1.1 (iso.3.6.1.2.1.1)
          Value (Null)
```

The image shows the 'Name Resolution' settings dialog in Wireshark. The 'Name Resolution' section is active, showing several options: 'Resolve MAC addresses' (checked), 'Resolve transport names' (unchecked), 'Resolve network (IP) addresses' (unchecked), 'Use captured DNS packet data for address resolution' (checked), 'Use an external network name resolver' (checked), and 'Use custom list of DNS servers for name resolution' (unchecked). Below these are fields for 'DNS Servers' (with an 'Edit...' button), 'Maximum concurrent requests' (set to 500), and several checkboxes for 'Only use the profile "hosts" file', 'Resolve VLAN IDs', and 'Resolve SS7 PCs'. A highlighted section contains 'Enable OID resolution' (unchecked) and 'Suppress SMI errors' (unchecked). At the bottom, there are fields for 'SMI (MIB and PIB) paths' and 'SMI (MIB and PIB) modules', both with 'Edit...' buttons, and 'MaxMind database directories' with an 'Edit...' button.



# Using included MIBs



Enable OID resolution  
 Suppress SMI errors

SMI (MIB and PIB) paths

SMI (MIB and PIB) modules

SMI Paths

Directory path

[/Users/sake/.config/wireshark/smi\\_paths](#)

SMI Modules

Module name

- IP-MIB
- IF-MIB
- TCP-MIB
- UDP-MIB
- SNMPv2-MIB
- RFC1213-MIB
- IPV6-ICMP-MIB
- IPV6-MIB
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-PROXY-MIB
- SNMP-TARGET-MIB
- SNMP-USER-BASED-SM-MIB
- SNMP-USM-DH-OBJECTS-MIB
- SNMP-VIEW-BASED-ACM-MIB

[/Users/sake/.config/wireshark/smi\\_modules](#)

No.	Time	Source	Destination	Protocol	Info
720	108.9288010...	x201.local	rtr-wan.ams.SYN-bit.voip	SNMP	get-next-request SNMPv2-MIB::system
721	108.9296557...	rtr-wan.ams.SYN-bit.voip	x201.local	SNMP	get-response SNMPv2-MIB::sysDescr.0
722	108.9301108...	x201.local	rtr-wan.ams.SYN-bit.voip	SNMP	get-next-request SNMPv2-MIB::sysDescr.0
				SNMP	get-response SNMPv2-MIB::sysObjectID.0
				SNMP	get-next-request SNMPv2-MIB::sysObjectID.0
				SNMP	get-response SNMPv2-MIB::sysUpTime.0
				SNMP	get-next-request SNMPv2-MIB::sysUpTime.0
				SNMP	get-response SNMPv2-MIB::sysContact.0
				SNMP	get-next-request SNMPv2-MIB::sysContact.0
				SNMP	get-response SNMPv2-MIB::sysName.0
				SNMP	get-next-request SNMPv2-MIB::sysName.0

Simple Network Management Protocol

- version: v2c (1)
- community: SYN-bit-public
- data: get-response (2)
  - get-response
    - request-id: 601920577
    - error-status: noError (0)
    - error-index: 0
    - variable-bindings: 1 item
      - SNMPv2-MIB::sysDescr.0 (1.3.6.1.2.1.1.1.0): Vyatta VyOS 1.1.8
        - Object Name: 1.3.6.1.2.1.1.1.0 (SNMPv2-MIB::sysDescr.0)
        - SNMPv2-MIB::sysDescr: Vyatta VyOS 1.1.8

[Response to: 720]  
[Time: 0.000854704 seconds]





# Adding specific MIBs



The top section shows two dialog boxes: 'SMI Paths' and 'SMI Modules'. The 'SMI Paths' dialog has a 'Directory path' field containing '/Users/sake/OneDrive - SYN-bit/sharkfest/sf21vus/presentation/mibs'. The 'SMI Modules' dialog lists several module names including SNMP-USER-BASED-SM-MIB, SNMP-USM-DH-OBJECTS-MIB, and PAN-COMMON-MIB. Both dialog boxes have 'Cancel' and 'OK' buttons. Two red warning boxes with exclamation marks are overlaid on the dialogs, stating 'Wireshark needs to be restarted for these changes to take effect'.

The bottom section shows a Wireshark packet capture window. The filter is '(snmp) && (ip.addr == 192.168.100.254)'. The packet list shows several SNMP messages. A red box highlights two specific packets: a 'get-next-request' for 'PAN-GLOBAL-REG::panCommonMib.2.2.1.0' and its corresponding 'get-response'. A red circle highlights the 'Enable OID resolution' checkbox (checked) and the 'Suppress SMI errors' checkbox (unchecked) in a dialog box. A tooltip for the 'Suppress SMI errors' checkbox explains: 'While loading MIB or PIB modules errors may be detected, which are reported. Some errors can be ignored. If unsure, set to false.' A 'Multiple problems found' error dialog is also visible, stating 'Stopped processing module RFC1213-MIB due to error(s) to prevent potential crash in libsmi.'

No.	Time	Source	Destination	Protocol	Info
1526	109.1315747...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-next-request SNMPv2-MIB::sysServices.0
1528	109.1320465...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-response SNMPv2-MIB::sysORLastChange.0
	109.1324705...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-next-request SNMPv2-MIB::sysORLastChange.0
	109.1340307...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-response IF-MIB::ifNumber.0
	109.1588770...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-next-request PAN-GLOBAL-REG::panCommonMib.2.2.1.0
	109.2063092...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-response PAN-GLOBAL-REG::panCommonMib.2.3.1.0
	109.2067569...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-request PAN-GLOBAL-REG::panCommonMib.2.2.1.0
	109.2081544...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-response PAN-GLOBAL-REG::panCommonMib.2.2.1.0
	109.2335311...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-next-request PAN-GLOBAL-REG::panCommonMib.2.1.1.0
	109.2359587...	x201.local	fw.dc.SYN-bit.voip	SNMP	get-response PAN-GLOBAL-REG::panCommonMib.2.1.2.0



# MIB errors?

Object Name	OID	Type	Access	Info
panCommonMibModule	1.3.6.1.4.1.25461.1.1.3			
panCommonConfMib	1.3.6.1.4.1.25461.2.1.1			
panCommonObjs	1.3.6.1.4.1.25461.2.1.2			
panSys	1.3.6.1.4.1.25461.2.1.2.1			
panSysSwVersion	1.3.6.1.4.1.25461.2.1.2.1.1	displaystring	read-only	
panSysHwVersion	1.3.6.1.4.1.25461.2.1.2.1.2	displaystring	read-only	
panSysSerialNumber	1.3.6.1.4.1.25461.2.1.2.1.3	displaystring	read-only	
panSysTimeZoneOffset	1.3.6.1.4.1.25461.2.1.2.1.4	integer32	read-only	
panSysDaylightSaving	1.3.6.1.4.1.25461.2.1.2.1.5	truthvalue	read-only	
panSysVpnClientVersion	1.3.6.1.4.1.25461.2.1.2.1.6	displaystring	read-only	
panSysAppVersion	1.3.6.1.4.1.25461.2.1.2.1.7	displaystring	read-only	
panSysAvVersion	1.3.6.1.4.1.25461.2.1.2.1.8	displaystring	read-only	
panSysThreatVersion	1.3.6.1.4.1.25461.2.1.2.1.9	displaystring	read-only	
panSysUrlFilteringVersion	1.3.6.1.4.1.25461.2.1.2.1.10	displaystring	read-only	
panSysHAState	1.3.6.1.4.1.25461.2.1.2.1.11	displaystring	read-only	
panSysHAPeerState	1.3.6.1.4.1.25461.2.1.2.1.12	displaystring	read-only	
panSysHAMode	1.3.6.1.4.1.25461.2.1.2.1.13	displaystring	read-only	
panSysUrlFilteringDatabase	1.3.6.1.4.1.25461.2.1.2.1.14	displaystring	read-only	
panSysGlobalProtectClientVersion	1.3.6.1.4.1.25461.2.1.2.1.15	displaystring	read-only	
panSysOpswatDatafileVersion	1.3.6.1.4.1.25461.2.1.2.1.16	displaystring	read-only	
panChassis	1.3.6.1.4.1.25461.2.1.2.2			
panChassisType	1.3.6.1.4.1.25461.2.1.2.2.1	displaystring	read-only	Chassis type for this Palo Alto device.

```
panChassisType OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Chassis type for this Palo Alto device."
    ::= { panChassis 1 }
```

```
variable-bindings: 1 item
  PAN-GLOBAL-REG::panCommonMib.2.2.1.0 (1.3.6.1.4.1.25461.2.1.2.1.0): Value (Null)
    Object Name: 1.3.6.1.4.1.25461.2.1.2.2.1.0 (PAN-GLOBAL-REG::panCommonMib.2.2.1.0)
```



Also: the module names need to match exactly so some MIB editing might be needed to make it work.





# Takeaways



- Out-of-the-box resolving works pretty good
  - Ignorance is bliss!
- There are unexpected glitches in the matrix
  - Take the red pill and dive deep
- Each protocol layers works just a little different, and there is unexpected behaviour
  - We need to fix this!!!
- The (reverse) name resolution system is pretty powerful when used correctly :-)







**SYN-bit**  
deep traffic analysis

**Application and network troubleshooting**

---

**Protocol and packet analysis**

---

**Training (Wireshark, TCP, SSL)**

**[www.SYN-bit.nl](http://www.SYN-bit.nl)**





# FIN/ACK/FIN/ACK



*If you have questions?*  
***sake.blok@SYN-bit.nl***



**SYN-bit**  
deep traffic analysis