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
Hello, what's your name? - An overview of Wireshark's name resolution options

$ whoami
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!

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)
Ignorance is bliss?

Hello, what's your name? - An overview of Wireshark’s name resolution options

https://flic.kr/p/8xhk74
By default:

- 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 GeoIP 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)

- `C:\Users\[username]\Documents\` (Documents)
- `C:\Users\[username]\AppData\Local\Temp\` (Temp)
- `C:\Users\[username]\AppData\Roaming\Wireshark\` (Personal configuration)
- `C:\Program Files\Wireshark\` (Global configuration)
- `C:\Program Files\Wireshark\plugins\` (Plugins)
- `C:\Program Files\Wireshark\plugins\3.4\` (Program Plugins)
- `C:\Program Files\Wireshark\plugins\3.4\` (Global Plugins)
- `C:\Program Files\Wireshark\plugins\` (Global Lua Plugins)
- `C:\Program Files\Wireshark\plugins\` (Personal Lua Plugins)
- `C:\Program Files\Wireshark\extcap\` (Personal Extcap path)
- `C:\Program Files\Wireshark\extcap\` (Global Extcap path)
- `C:\Program Files\Wireshark\GeoIP\` (MaxMind DB path)
- `C:\Program Files\Wireshark\GeoIP\` (MaxMind DB path)
- `C:\Program Files\Wireshark\GeoIP\` (MIB/PIB path)

Typical Files:
- capture files
- untitled capture files
- filters, preferences, ethers...
- etc., ipnets
- program files
- binary plugins
- lua scripts
- Extcap Plugins search path
- MaxMind DB database search path
- MIB/PIB search path

Hello, what's your name? - An overview of Wireshark's name resolution options
# File locations (MacOS)

## Filter by path

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Typical Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;File&quot; dialogs</td>
<td><code>/Users/aake/</code></td>
<td>capture files</td>
</tr>
<tr>
<td>Extcap path</td>
<td><code>/Applications/Wireshark-3.5.0.app/Contents/MacOS/extcap</code></td>
<td>Extcap Plugins search path</td>
</tr>
<tr>
<td>Global Lua Plugins</td>
<td><code>/Applications/Wireshark-3.5.0.app/Contents/Plugins/wireshark</code></td>
<td>lua scripts</td>
</tr>
<tr>
<td>Global Plugins</td>
<td><code>/Applications/Wireshark-3.5.0.app/Contents/Plugins/wireshark/3-5</code></td>
<td>binary plugins</td>
</tr>
<tr>
<td>Global configuration</td>
<td><code>/Applications/Wireshark-3.5.0.app/Contents/Resources/share/wireshark</code></td>
<td>dfilters, preferences, manuf, ...</td>
</tr>
<tr>
<td>MIB/PIB path</td>
<td><code>/usr/share/GeoIP</code></td>
<td>SMI MIB/PIB search path</td>
</tr>
<tr>
<td>MaxMind DB path</td>
<td><code>/var/lib/GeoIP</code></td>
<td>MaxMind DB database search path</td>
</tr>
<tr>
<td>MaxMind DB path</td>
<td></td>
<td>MaxMind DB database search path</td>
</tr>
<tr>
<td>Personal Extcap path</td>
<td><code>/Users/aake/.config/wireshark/extcap</code></td>
<td>Extcap Plugins search path</td>
</tr>
<tr>
<td>Personal Lua Plugins</td>
<td><code>/Users/aake/.local/lib/wireshark/plugins</code></td>
<td>lua scripts</td>
</tr>
<tr>
<td>Personal Plugins</td>
<td><code>/Users/aake/.local/lib/wireshark/plugins/3-5</code></td>
<td>binary plugins</td>
</tr>
<tr>
<td>Personal configuration</td>
<td><code>/Users/aake/.config/wireshark</code></td>
<td>dfilters, preferences, others, ...</td>
</tr>
<tr>
<td>Program</td>
<td><code>/Applications/Wireshark-3.5.0.app/Contents/MacOS</code></td>
<td>program files</td>
</tr>
<tr>
<td>System</td>
<td><code>/etc</code></td>
<td>others, ipxnets</td>
</tr>
<tr>
<td>Temp</td>
<td><code>/var/folders/8/69n1j2nd2bxqi0390tsf1tcp7w00000gn/T</code></td>
<td>untitled capture files</td>
</tr>
<tr>
<td>macOS Extras</td>
<td><code>/Applications/Wireshark-3.5.0.app/Contents/Resources/Extras</code></td>
<td>Extra macOS packages</td>
</tr>
</tbody>
</table>
Hello, what's your name? - An overview of Wireshark's name resolution options
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
Hello, what's your name? - An overview of Wireshark's name resolution options
VLAN Resolution Process

1. Does the file "vlans" exist in the configuration profile?
   - Yes: Use the name from the entry in the vlans file in the configuration profile.
   - No: Does the file "vlans" exist in the default profile?
     - Yes: Use the name from the entry in the vlans file in the default profile.
     - No: Is the VLAN ID listed in the vlans file in the configuration profile?
       - Yes: Use the name from the entry in the vlans file in the configuration profile.
       - No: Use <vlan_id>.
• 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?)
Hello, what's your name? - An overview of Wireshark's name resolution options
Transport Resolution Process

START

Does the file "services" exist in the configuration profile?

yes → Is the port number listed in the services file in the configuration profile?

yes → Use the name from the entry in the services file in the configuration profile

no → no

Is the file "services" exist in the default profile?

yes → Is the port number listed in the services file in the default profile?

yes → Use the name from the entry in the services file in the default profile

no → no

Is the port number listed in the services file in the global preferences directory?

yes → Use the name from the entry in the services file in the global configuration directory

no → Show the port number instead of a name
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?)
• 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)

manuf file???
When "Use captured DNS packet data for address resolution" is enabled
Hello, what's your name? - An overview of Wireshark's name resolution options

Does not seem to be implemented (yet?)
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
example - hosts

Hello, what's your name? - An overview of Wireshark's name resolution options
Hello, what's your name? - An overview of Wireshark's name resolution options
Hello, what's your name? - An overview of Wireshark's name resolution options
Hello, what's your name? - An overview of Wireshark's name resolution options
Hello, what's your name? - An overview of Wireshark's name resolution options
Hello, what's your name? - An overview of Wireshark's name resolution options
Hello, what's your name? - An overview of Wireshark's name resolution options

#SF21VUS / @SYNbit
Hello, what's your name? - An overview of Wireshark’s name resolution options
Hello, what's your name? - An overview of Wireshark’s name resolution options

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
Wireshark can use GeoLite2 databases

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:
Configuring MMDB Paths

Hello, what's your name? - An overview of Wireshark's name resolution options
GeoIP example

Ethernet II, Src: x201.local (10:0e:71:58:72:05),Dst: rtr-lan-tel.str-201.101p (00:0c:29:00:cf:16)

802.1Q Virtual LAN, PRI: 0, DEI: 0, VID: 112

IPv4 Protocol Version 4, Src: x201.local (10.0.112.103), Dst: one.one.one.one (1.0.0.1)

- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: DSCP: CS0, ECN: Not-ECT
- Total Length: 84
- Identification: 0x085a (51290)
- Flags: 0x40, Don't fragment
- Time to Live: 64
- Protocol: ICMP (1)
- Header Checksum: 0x6f66 [validation disabled]
- 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
Using included MIBs

- Enable OID resolution
- Suppress SMI errors

**SMI Paths**

- Directory path: /Users/saker/config/wireshark/smi_paths

**SMI Modules**

- Simple Network Management Protocol

- Version: v2c (1)
- Community: SYN-bit-public
- Data: get-response (2)
- get-response
  - request-id: 601928577
  - error-status: noError (0)
  - error-index: 0
- variable-bindings: 1 item
  - SNMPv2-MIB::sysDescr.0: Vyatta VyOS 1.1.8
  - SNMPv2-MIB::sysOperStatus: 1.3.6.1.2.1.1.1.0
  - SNMPv2-MIB::sysObjectID: 1.3.6.1.2.1.1.1.0
- get-next-request SNMPv2-MIB::system

**Hello, what's your name? - An overview of Wireshark's name resolution options**
Hello, what's your name? - An overview of Wireshark's name resolution options
MIB errors?

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 :-)

#SF21VUS / @SYNbit
Application and network troubleshooting

Protocol and packet analysis

Training (Wireshark, TCP, SSL)

www.SYN-bit.nl
If you have questions?

sake.blok@SYN-bit.nl