## NAME

extcap − The extcap interface

## DESCRIPTION

The extcap interface is a versatile plugin interface that allows external binaries to act as capture interfaces directly in Wireshark. It is used in scenarios, where the source of the capture is not a traditional capture model (live capture from an interface, from a pipe, from a file, etc). The typical example is connecting esoteric hardware of some kind to the main Wireshark application.

Without extcap, a capture can always be achieved by directly writing to a capture file:

```
the−esoteric−binary −−the−strange−flag −−interface=stream1 −−file dumpfile.pcap &
wireshark dumpfile.pcap
```

but the extcap interface allows for such a connection to be easily established and configured using the Wireshark GUI.

The extcap subsystem is made of multiple extcap binaries that are automatically called by the GUI in a row. In the following chapters we will refer to them as "the extcaps".

Extcaps may be any binary or script within the extcap directory. Please note, that scripts need to be executable without prefacing a script interpreter before the call.

WINDOWS USER: Because of restrictions directly calling the script may not always work. In such a case, a batch file may be provided, which then in turn executes the script. Please refer to doc/extcap_example.py for more information.

When Wireshark launches an extcap, it automatically adds its installation path (c:\Program Files\Wireshark\) to the DLL search path so that the extcap library dependencies can be found (it is not designed to be launched by hand). This is done on purpose. There should only be extcap programs (executable, python scripts, ...) in the extcap folder to reduce the startup time and not have Wireshark trying to execute other file types.

## GRAMMAR ELEMENTS

Grammar elements:

arg (options)

argument for CLI calling

number

Reference # of argument for other values, display order

call

Literal argument to call (−−call=...)

display

Displayed name

default

Default value, in proper form for type

range

Range of valid values for UI checking (min,max) in proper form

type

Argument type for UI filtering for raw, or UI type for selector:

```
integer
unsigned
long (may include scientific / special notation)
float
selector (display selector table, all values as strings)
boolean (display checkbox)
radio (display group of radio buttons with provided values, all values as stri
fileselect (display a dialog to select a file from the filesystem, value as st
multicheck (display a textbox for selecting multiple options, values as string
password (display a textbox with masked text)
timestamp (display a calendar)
```

value (options)

```
Values for argument selection
arg     Argument # this value applies to
```

## EXAMPLES

Example 1:

```
arg {number=0}{call=--channel}{display=Wi-Fi Channel}{type=integer}{required=true
arg {number=1}{call=--chanflags}{display=Channel Flags}{type=radio}
arg {number=2}{call=--interface}{display=Interface}{type=selector}
value {arg=0}{range=1,11}
value {arg=1}{value=ht40p}{display=HT40+}
value {arg=1}{value=ht40m}{display=HT40-}
value {arg=1}{value=ht20}{display=HT20}
value {arg=2}{value=wlan0}{display=wlan0}
```

Example 2:

```
arg {number=0}{call=--usbdevice}{USB Device}{type=selector}
value {arg=0}{call=/dev/sysfs/usb/foo/123}{display=Ubertooth One sn 1234}
value {arg=0}{call=/dev/sysfs/usb/foo/456}{display=Ubertooth One sn 8901}
```

Example 3:

```
arg {number=0}{call=--usbdevice}{USB Device}{type=selector}
arg {number=1}{call=--server}{display=IP address for log server}{type=string}{val
flag {failure=Permission denied opening Ubertooth device}
```

Example 4: arg {number=0}{call=--username}{display=Username}{type=string} arg {number=1}{call=--password}{display=Password}{type=password}

Example 5: arg {number=0}{call=--start}{display=Start Time}{type=timestamp} arg {number=1}{call=--end}{display=End Time}{type=timestamp}

## SECURITY AWARENESS

- Users running wireshark as root, we can’t save you
- Dumpcap retains suid/setgid and group+x permissions to allow users in wireshark group only
- Third−party capture programs run w/ whatever privs they’re installed with
- If an attacker can write to a system binary directory, we’re game over anyhow
- Reference the folders tab in the wireshark→about information, to see from which directory extcap is being run

## SEE ALSO

wireshark(1), tshark(1), dumpcap(1), androiddump(1), sshdump(1), randpktdump(1)

## NOTES

**Extcap** is feature of **Wireshark**. The latest version of **Wireshark** can be found at https://www.wireshark.org.

HTML versions of the Wireshark project man pages are available at https://www.wireshark.org/docs/man−pages.