Using Wireshark with the CloudShark Plug-in
Monday June 25th 2012

Joe McEachern
CEO and Founder | CloudShark

Zach Chadwick
Lead Developer | CloudShark

WARNING: This presentation may be interactive! Start packet surfing right from your seat!

@cloudshark

https://surf.cloudshark.org
User: sharkfest
Password: sharkfest
Act One: The Evolution of CloudShark

“We’re going to need a bigger boat!”
-- Jaws, 1975
In the Beginning ...

It all started at QA Cafe in Portsmouth, New Hampshire, USA …

qa cafe
ip test solutions

… We develop CDRouter for testing CPE devices (aka gateways, routers, edge devices).

CDRouter

… Our test software has probably been used to test the router in your home.

… Lots of packets, lots of Wireshark
# Act One: The CloudShark Story

## The CloudShark Timeline

<table>
<thead>
<tr>
<th>Year</th>
<th>Events</th>
</tr>
</thead>
</table>
| 2010 | - QA Cafe developed technology to view packets in the web  
- We called it “inline packet decode” Sexy!  
- We wanted to make this capability available to a wider audience  
- Launched free CloudShark.org |
| 2011 | - What about security in the cloud?  
- “Pushing packets to the cloud is a dumb idea!”  
- Okay, here is the CloudShark appliance. Deploy it in your own network! |
| 2012 | - Still using Wireshark to create captures.  
- Let’s make it easier to send your capture files from Wireshark to CloudShark  
- Released a GPL Wireshark plug-in that makes it easier to send captures to CloudShark |
Act Two: Quick Tour of CloudShark

“You got any better suggestions”
-- Jaws, 1975
Why CloudShark?

• How things were done B.C.

• “Before CloudShark”
Why CloudShark?

- “Hey can you look at something?”
- Sticky Fingers
- BLT not TCP
- SneakerNet
Why CloudShark?

https://www.cloudshark.org/captures/f62e1db77ba0
Why CloudShark?

- Store
- View
- Analyze
- Annotate
- Share
Why CloudShark?
Why CloudShark?

• Centralized storage
Why CloudShark?

• Now where did I put that....?
• Indexes the metadata
• Searching
Quick Demo

Start packet surfing right from your seat!

@cloudshark

https://surf.cloudshark.org
User: sharkfest
Password: sharkfest
Why CloudShark?

• How do we make this even easier?
• It’s plugin time!
Act Three: Getting Started with the Plugin

“That’s some bad hat Harry”
-- Jaws, 1975
Wireshark Plug-in

- The plug-in uses Wireshark’s Lua plug-in interface.
- Once installed, the Tools menu is extended with a new CloudShark option.
- Use the Upload option to push the current capture file to CloudShark.
- Wireshark opens the default browser with a CloudShark session URL.

View from Web
Installation

- Download free installer from cloudshark.org. Latest version is 1.0.1.
- Installers available for Windows, OSX, and generic unix (*.tgz).
- Installed under user’s Wireshark plugins directory (platform specific).
- Simply restart Wireshark and plug-in is detected automatically.
Configuration

- Text based configuration available from CloudShark menu
- Configure CloudShark URL to CloudShark.org or your own appliance
- Setup API key, user, password
- Setup additional tags
- Certificate configuration for curl

```bash
-- URL: The CloudShark appliance URL
CLOUDSHARK_URL = "https://www.cloudshark.org"

-- API: The API token to use
CLOUDSHARK_API_KEY = "59f5893a534b9d1bb2c9587a5e508"

-- Tags: A comma separated list of tags
CLOUDSHARK_TAGS = ""

-- User: The user name (only if login is required)
CLOUDSHARK_USER = ""

-- Password: The password (only if login is required)
CLOUDSHARK_PASSWORD = ""

-- Tshark: To enable tshark support for the plugin.
-- set the CLOUDSHARK_TSHARK setting to "y" for auto
-- node or "prompt" for prompting mode.
CLOUDSHARK_TSHARK = "n"

-- Curl: The path to curl if non-standard
-- Paths should be formatted with [[path]]
-- Remove the -- below to uncomment
-- CLOUDSHARK_CURL = [[C:\example\curl.exe]]

-- CA Bundle: The path to an alternative CA bundle file in pem format
-- Paths should be formatted with [[path]]
-- Remove the -- below to uncomment
-- CLOUDSHARK_CABUNDLE = [[C:\example\curl-ca-bundle.crt]]
```

Save Close
Wireshark Plug-in

- Works with live capture or stoppedloaded capture.
- Upload sends capture to CloudShark web API using https POST.
- Plug-in checks response and determines CloudShark session URL.
Live Plug-in Examples

Start surfing now. Sample captures will be uploaded to surf.cloudshark.org.

@cloudshark
https://surf.cloudshark.org
User: sharkfest
Password: sharkfest
Act Four: Using the Plug-in with tshark

“This was no boat accident”
-- Jaws, 1975
Using the Plug-In with tshark

- User interface challenge
- Off by default
- Can enable automatic uploads or prompting through Cloudshark preferences file
- Great for scripting and automation tools
- CloudShark session URL displayed in tshark output
Live Tshark Examples

Here come some more waves. Grab your board and head to surf.cloudshark.org.

@cloudshark

https://surf.cloudshark.org
User: sharkfest
Password: sharkfest
Act Five: Setting up for the Plug-in

“Come on into the water.”
-- Jaws, 1975
Setting up for the Plugin

1. Create Token
2. Settings
3. Copy/Paste

API Token: d02fd17392176a29e98ac7d40ef17c59
Act Six: A quick look under the hood

This shark, swallow you whole.
-- Jaws, 1975
• Lua provides cross platform support
• How do you get Wireshark to speak web? Use combination of Curl and Lua JSON library.
• Not many Wireshark GUI controls available through Lua – but enough!
• Support tshark by detecting GUI.
• Go deeper in Wednesday’s Sharkfest session.
Act Seven: Lessons Learned

*What we have here is a eating machine.*
-- Jaws, 1975
Lessons Learned: Uploads

- No signups
- No logins
- No limit to imagination of uploads!
Lessons Learned: Uploads

- MP3
- MPEG
- JPEG

Historical reasons for support?
Lessons Learned: Uploads

- Exploits
- Denial Of Service
- Sandbox
Lessons Learned: Mobile

• “Out of the office”

*standard data and messaging rates may apply
Lessons Learned: Data Size

- Bandwidth issues
- Too much data
- Information without all the data
- Caching
Lessons Learned: Community

- Great community
- PacketLife.org
- ask.wireshark.org
- SharkFest!
Act Eight: Wrapping up

Any special questions?
-- Jaws, 1975
Wrapping up

• Learn to packet surf today! Download the plugin now from cloudshark.org
• Login to https://surf.cloudshark.org
  user: sharkfest
  password: sharkfest
• Try out our capture challenge for Sharkfest attendees!
• Come back for Wednesday’s 11:00 session
  “Using Lua to implement the Wireshark Plug-in”

Have a great Sharkfest!