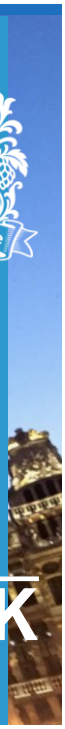
SharkFest'26 Europe

How to find problems quickly in a trace file (and win the packet challenge)

Eddi Blenkers



Sponsored by: PROFI TAP DEEP NETWORK OBSERVABILITY, cPacket, TCP/IP training, endace Record. Respond.

1

The esPCAPe Packet Challenge

- The Packet Challenge is a well-honoured tradition for Sharkfests.
- The winning team takes home prestige, medals, prices and unlimited bragging rights

- Some challenges are hair raising …
  - At least while the challenge is running
  - Given time and using the right Wireshark features they are very well solvable

- Here is your guide, so that *you* take home the big price

2

The Mission

- This year, you have to regain control of a damaged space craft
- As usual, the mission is a **team effort**

- This event is a bit of network forensics

https://www.stellar-bluetani.space/ctf/

3

What this talk is about

- Learn the most important Wireshark techniques to complete the mission.
  - Time is a factor in the challenge: Faster teams get a better ranking

- Network analysis as team effort
  - We often work alone on a trace file.
  - Working as a team requires some coordination

4

Important Wireshark Techniques

5

Export Objects

- Wireshark has a powerful feature to recover files and messages, that been transferred over the network
- **File → Export Objects**
  - Choose all relevant protocols
  - Start exploring to see, which protocols carry a file
  - Use **Statistics → Protocol Hierarchy** to identify protocols
- Special Info for the packet challenge:
  - Every protocol counts
  - There is only very little background noise

6

Find Information

- Use **Edit → Find Packet** to search for interesting packets
  - Even faster, with **Ctrl-F**
- Search for packets matching a display filter, or strings
  - Strings can be in the Packet List, Packet Details (decode) or in the raw bytes
  - Search-Strings can be 8 bit (ASCII) or wide (UTF-16)
  - Search can case-blind to observer capitalization
  - Go deep: Search for hex values or a regular expression
- Super useful in a case, where you know or guess a keyword

Protocol Preferences

- Configure TCP and TLS to reassemble streams
- Menu: **Edit → Preferences → Protocols**
- Configure TCP:
  - **Allow subdissector to to reassemble TCP stream**
  - **Reassemble out-of-order segments**
- Configure TLS:
  - **Reassemble TLS records spanning multiple TCP segments**
  - **Reassemble TLS Application Data spanning multiple TLS records**
  - specify the **(Pre)-Master-Secret log filename**

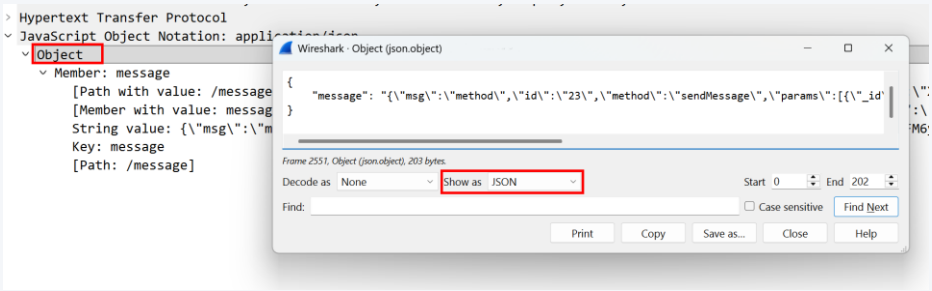
How to Decode TLS at Home

- First of all: This only works if OpenSSL is involved
  - Chrome, Firefox, Thunderbird use OpenSSL
  - Edge uses the Microsoft component **SChannel**, not OpenSSL
- Explain to your boss, your users and your privacy officer what you plan
  - Never do this without explicit user consent
  - Tell users to stay away from sites with confidential data:
    No home banking, no payroll, no insurance, do not search for health-related issues etc.
- Set the environment variable SSLKEYLOGFILE
  - **export SSLKEYLOGFILE=/tmp/sslkeys.log**
- Configure Wireshark to use the key file
  Edit → Preferences → Protocols → TLS and specify the **(Pre)-Master-Secret log filename**

9

Show Packet Bytes and Export Packet Bytes

- Right-Click on a decode line



- Make sure to click a line that makes sense
- Note that you can save the decoded information
- You might also try **Export Packet Bytes** for non-printable data

10

Use Comments (pcapng traces only)

- Traces in pcapng format can carry comments for the file and for each packet
- Comments for the capture file:
  - **Statistics → Capture File Properties → Edit Comments**
  - Supports multiple comments
  - Make notes on the problem, how the trace was recorded, important information etc.
- Use packet comments to note important conclusions
  - Right-Click to get a popup men, then select **Packet Comments**
  - DHCP indicates a device is booting
  - DNS requests shows the first connection to a server
  - First occurrence of a sequence number, that is later retransmitted
  - Change in network topology

Use AI?

- First of all, you are here to learn about Wireshark, not to learn prompting
- Then again: In these days, we use AI a lot …
  - Practice your prompting skills: What you get is what you prompt …
  - During our test runs, we noticed a few occasions where AI screwed up
- We have an idea, how AI-usage looks on our admin panel.
- **We stop handing out hints to a team, when we see signs of AI usage**

Wireshark as Team Sports

13

Building a Team

- Good start: The guys from your dinner table
- Use dinner conversation to get to know your team members

- Wireshark related topics:
  - Have you been to a Sharkfest before?
  - How long are you in networking?
  - How often do you use Wireshark?
  - What was your hardest / easiest / most remarkable troubleshooting session?
  - **What epic name should we choose for our epic team?**

- If Wireshark topics run dry:
  - Where are you from?
  - Where did you spend your last vacation?
  - What company are you working for?
  - Do you have kids?
  - Do you play an instrument?

14

Who is in a winning team?

- Mixed skill level: Rookie to seasoned sharkhead or core developper
- Rookies might feel out-of-place
  - Don't worry, you will take a very critical role
  - Surf through the trace file and see what comes up
  - Use the opportunity to learn: Note how display filters get longer, how data is dug up by other team members
- Some senior engineers tend to be quiet
  - Head bent over the screen or keyboard, occasionally mumbling a protocol name
  - Please, pretty please: Share you experience.
  - Let others know, what you are looking at

Assign Roles

- Investigator
  - Examine trace files to find clues.
  - Announce findings
  - Findings could be: Interesting protocols, messages, files
  - Share a display filter or click-sequence to reproduce the finding
- Librarian or Archivar
  - Collects all files and messages found by the team members
  - Reads all files and message. Top to bottom.
  - Documents all findings
  - Reads all files and message. Top to bottom. Read again.
- All team members
  - Discuss where to apply your findings.

More Roles: Ideas for Real-world Scenarios

- Logistics & Support
  - Arrange span ports, disk space, coffee, food, and more
  - Deal with the bureaucratic worlds in a large company
- Lead Investigator / Ambassador
  - Arrange short meetings where everyone gives a short account of current findings and activities
  - Make sure the investigation stays focussed.
    Don't deal with bandwidth problems in the remote office, when your data-center is out
  - Keep management informed (only with confirmed findings)
  - Keep management from micro-managing
    "No investigation into e-Mail unless I have approved each TCP session individually"

Working as a Team

- None of us ever had to recover a run-away space craft.
  - Therefore, we all make mistakes
  - Think like a football / soccer team: Not every attack results in a goal
- The challenge creates some time pressure
  - Ignore the clock. If you can.
  - Practice slow breathing, if you feel stressed.
- Communicate. Talk. Share notes, display filters and more.
  - Exchange ideas how to tackle a problem.
  - Every idea could bring the team a step closer to the big price.
- Treat each other with respect. Always.

Helpful Tools

- Use a web site to share information
  - Teams whiteboard, Etherpad, Mindwendel …
  - Note wrong answers. If possible: Note, what went wrong
- Share display filters or mouse-click sequences to get an important result
- Share passwords and other critical information.
  - But keep your voice down: Your neighbours are also searching.

General Tipps

- Answers can be found sequentially.
  - Packets to answers the first challenge come first in the trace.
  - Followed by packets to solve the second challenge …
- The web site treats you as a team:
  - One team member answering the correct question rewards the whole team.
  - One team member giving a wrong answer, … Well, you don't want that!
- Read all files and message. Top to bottom.
- Don't guess. Guessing will cost you valuable time. Literally.

Pre-Briefing

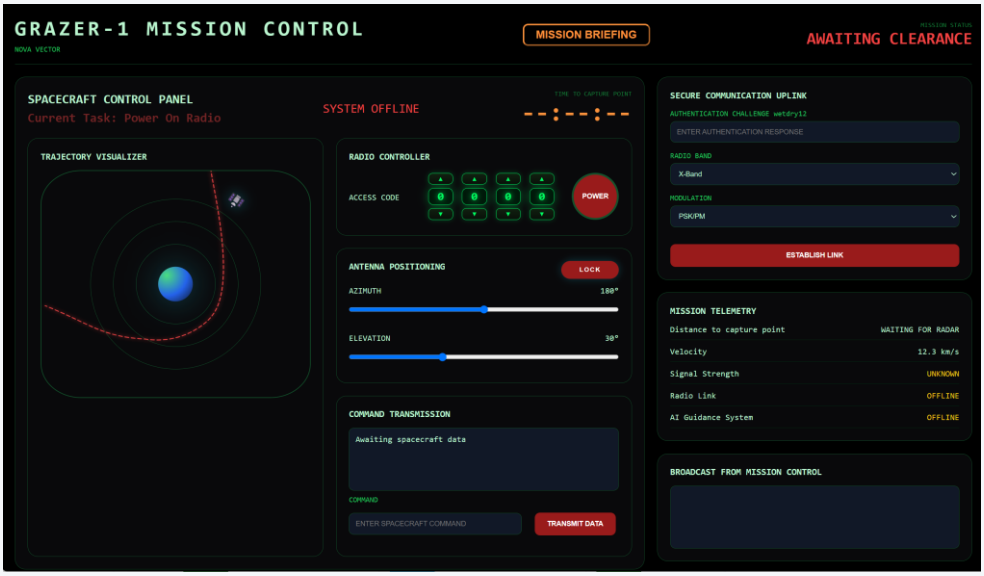
21

Your Mission

- The company **Stellar Bluetani** is currently leading the space race.
- Their latest product is an autonomous probe, that collects rare minerals from the asteroid belt.
- The whole world is watching, while the first probe, **GRAZER-1**, is approaching earth.
- Unfortunately, the navigation module has been disabled by a micro meteor
- The engineers who build the control panel are no longer with the company.
- It's up to you to bring the space probe into a stable orbit
- All that's left is an old trace file, that holds information to control the space probe

22

The Web Site



23

Practical Hints

- You need 4 steps to take control of the space craft
- If one team member provides a correct solution, the whole team gets promoted to the next question
- If one team member is caught doing something bad, the whole team will catch the consequences.
- Probe Security is



24

The Mission

- This year, you have to regain control of a damaged space craft
- The web site:

https://www.stellar-bluetani.space/ctf/

- On the web site you find
  - A trace file (encrypted, password will follow)
  - The mission briefing
  - A link to the registration page
  - No new team registration, after the mission starts

25

Thank You!

WIRESHARK

Your Feedback:

26