NetRipper – Smart traffic sniffing for penetration testers

Ionut Popescu – Senior Application Security Engineer @ 1&1 Romania

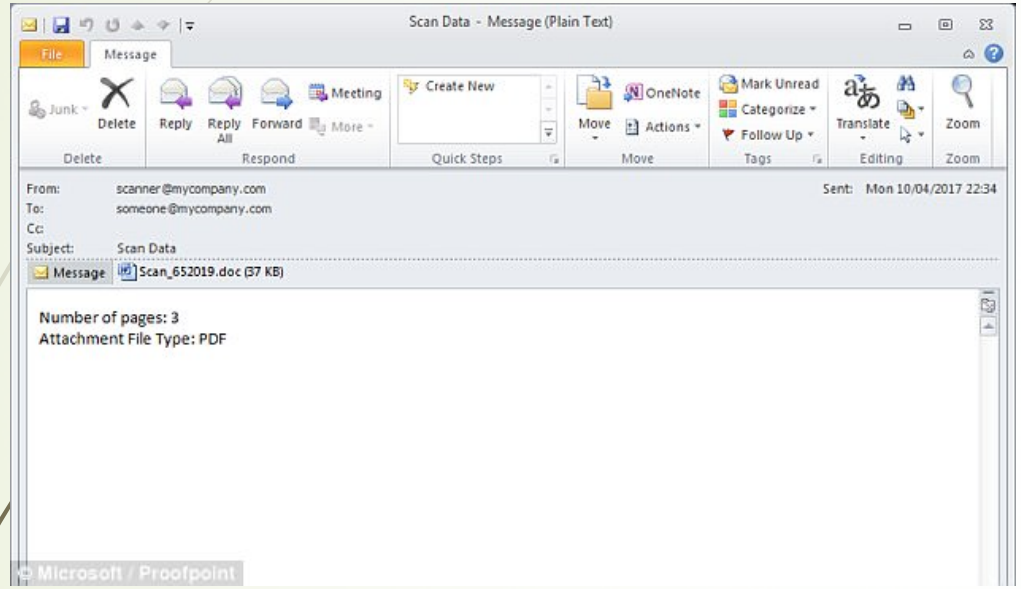
About me

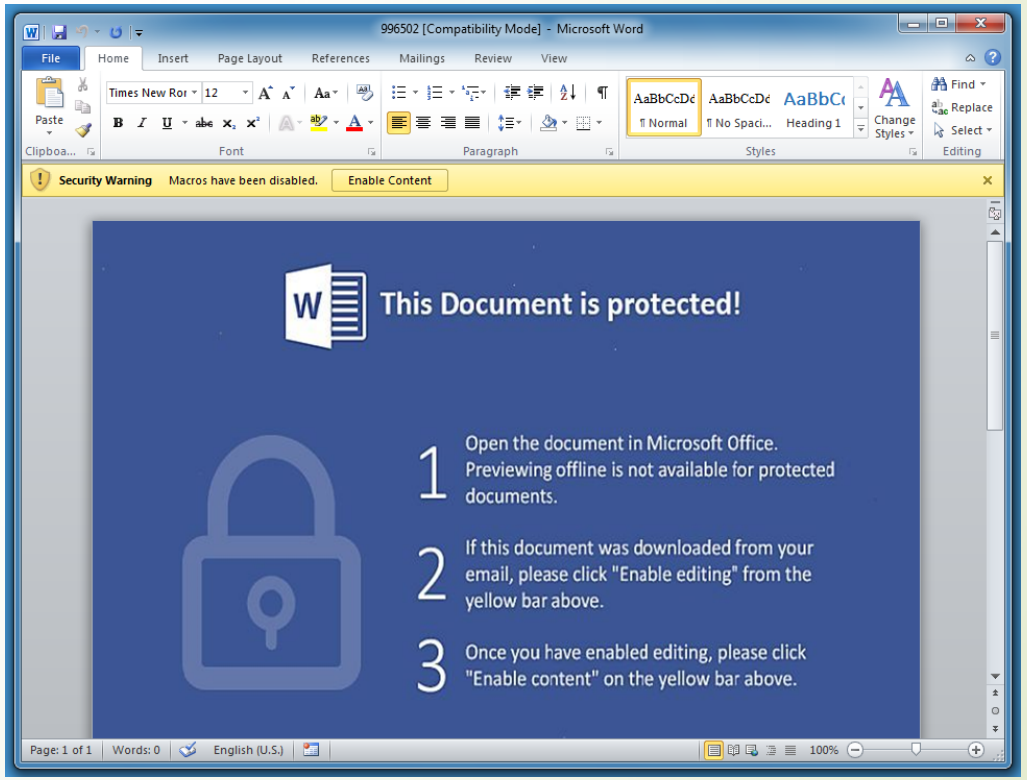
- Blogger @ https://nytrosecurity.com/
- GitHub @ https://github.com/NytroRST
- Twitter @ https://twitter.com/NytroRST
- Admin @ https://rstforums.com/forum/

NetRipper

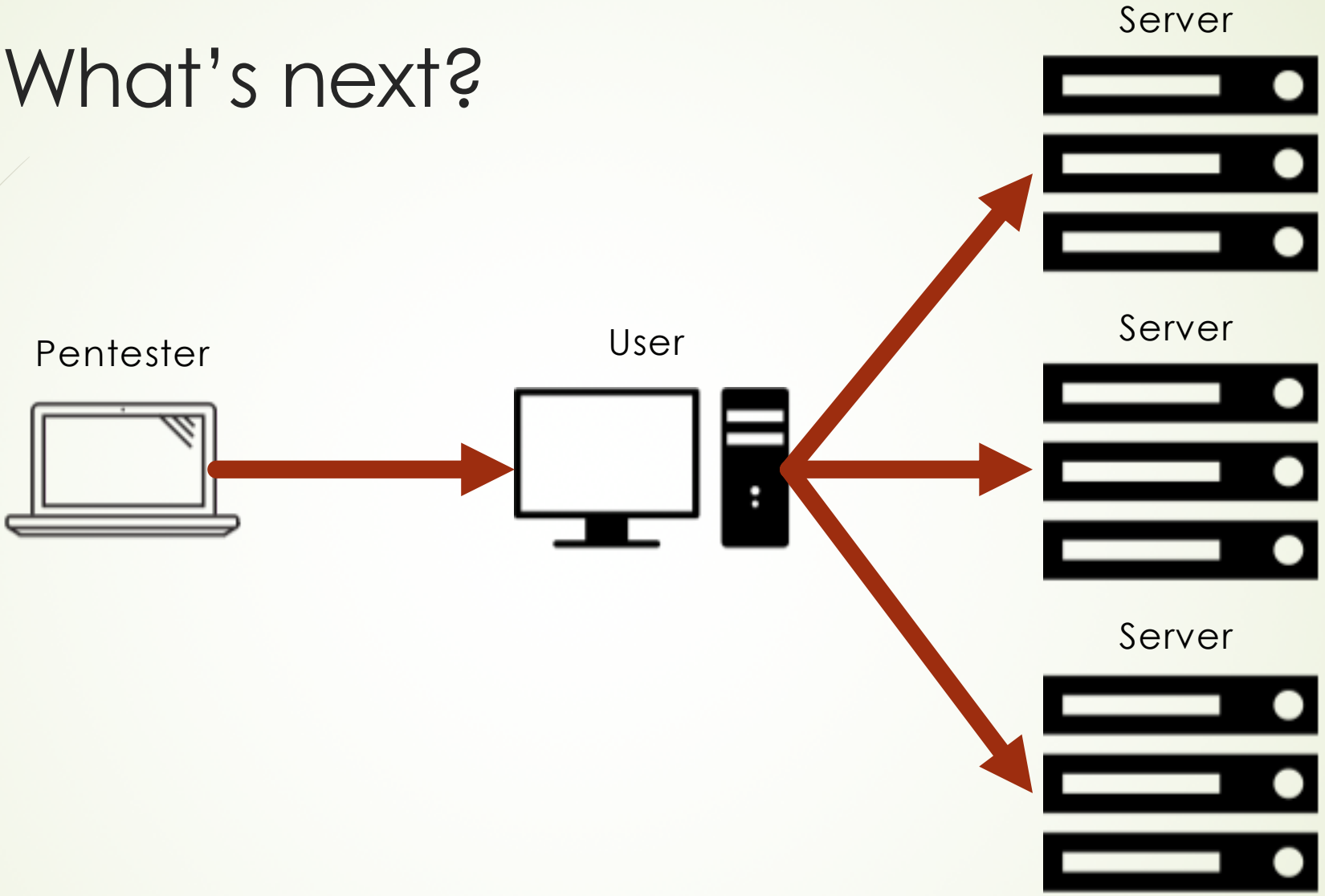
- Personal project
- Released at Defcon 23 (2015)
- Presented at BlackHat Asia Arsenal (2018)
- For penetration testers
- For anyone

Getting access to a workstation



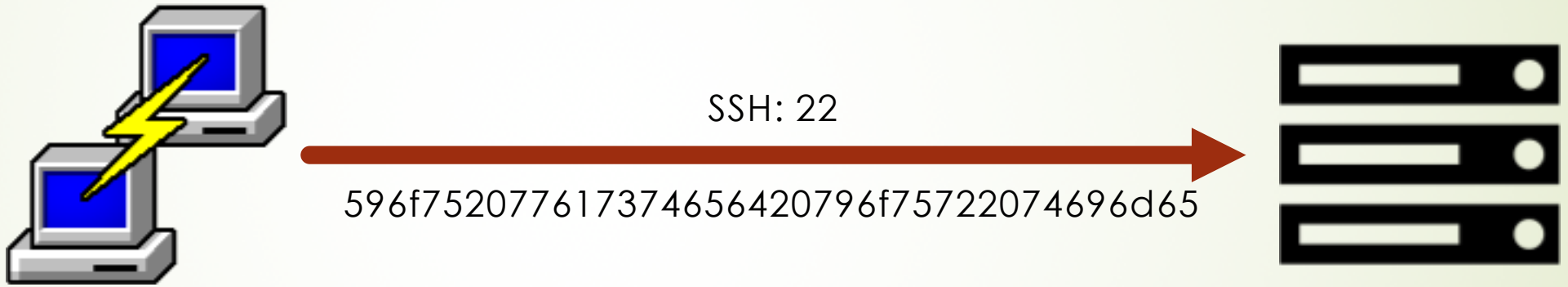


What's next?

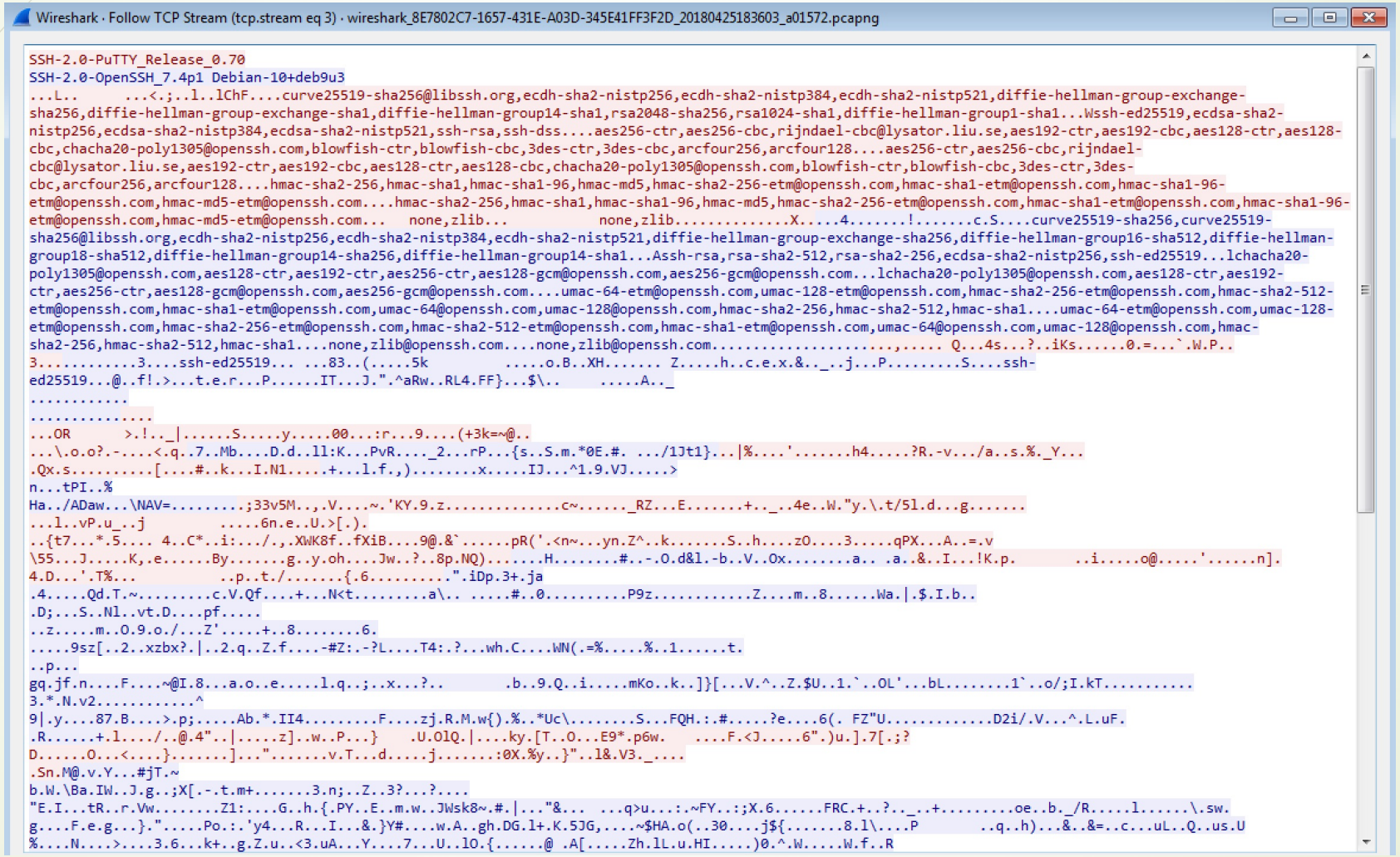


How to connect to servers?

Connection example

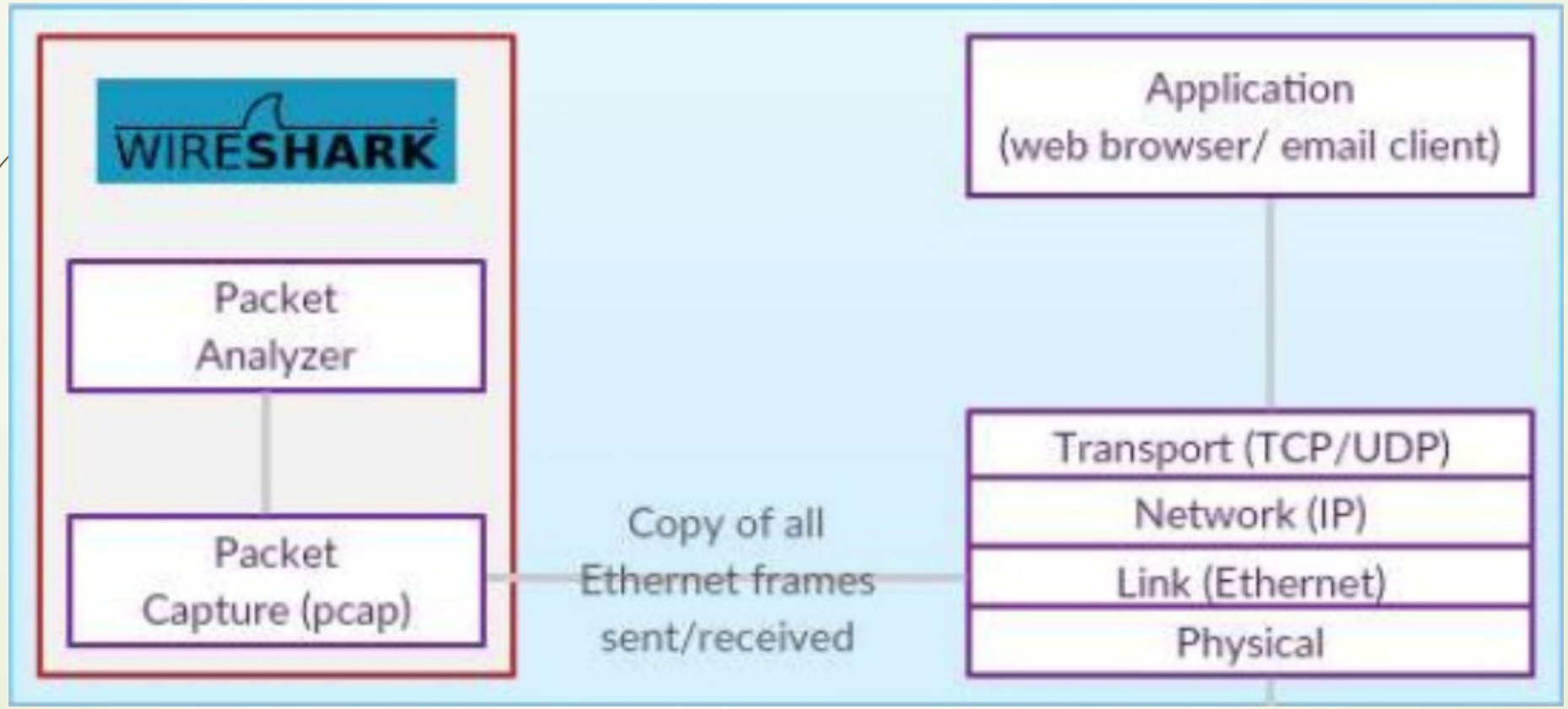


Traffic sniffing

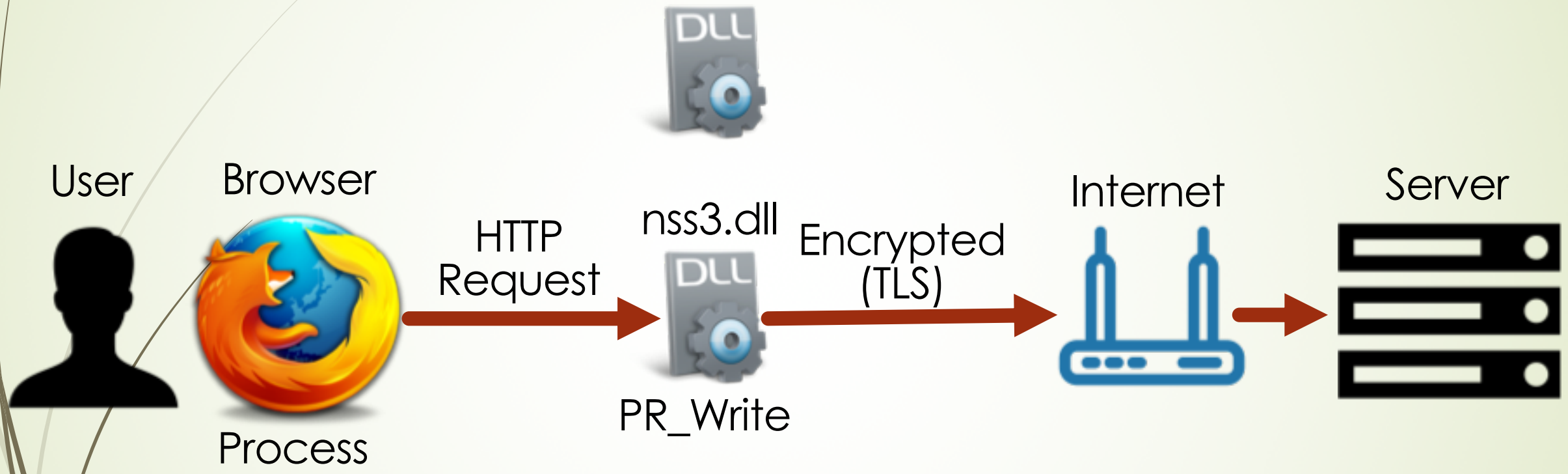


How a sniffer works

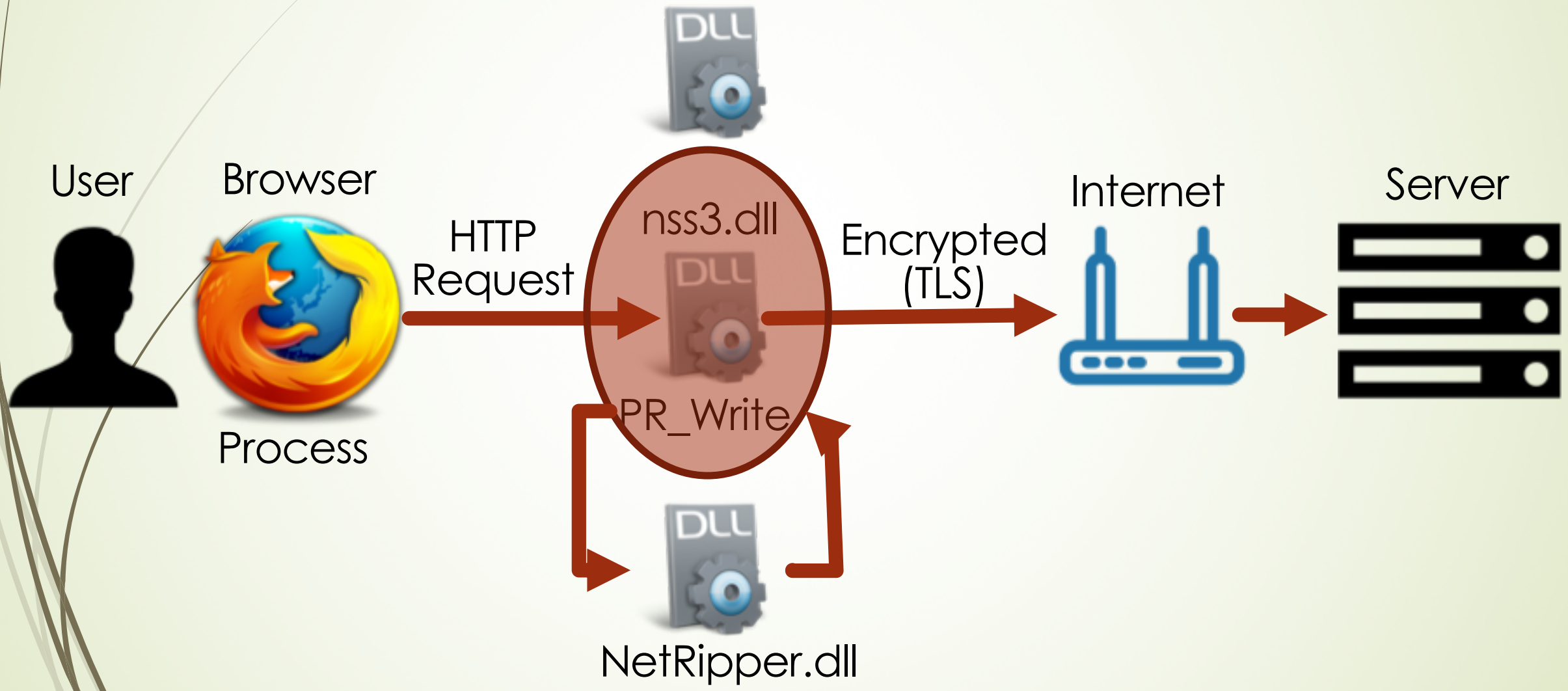
- It requires administrative privileges
- Useless for encrypted data (e.g. HTTPS, SSH)



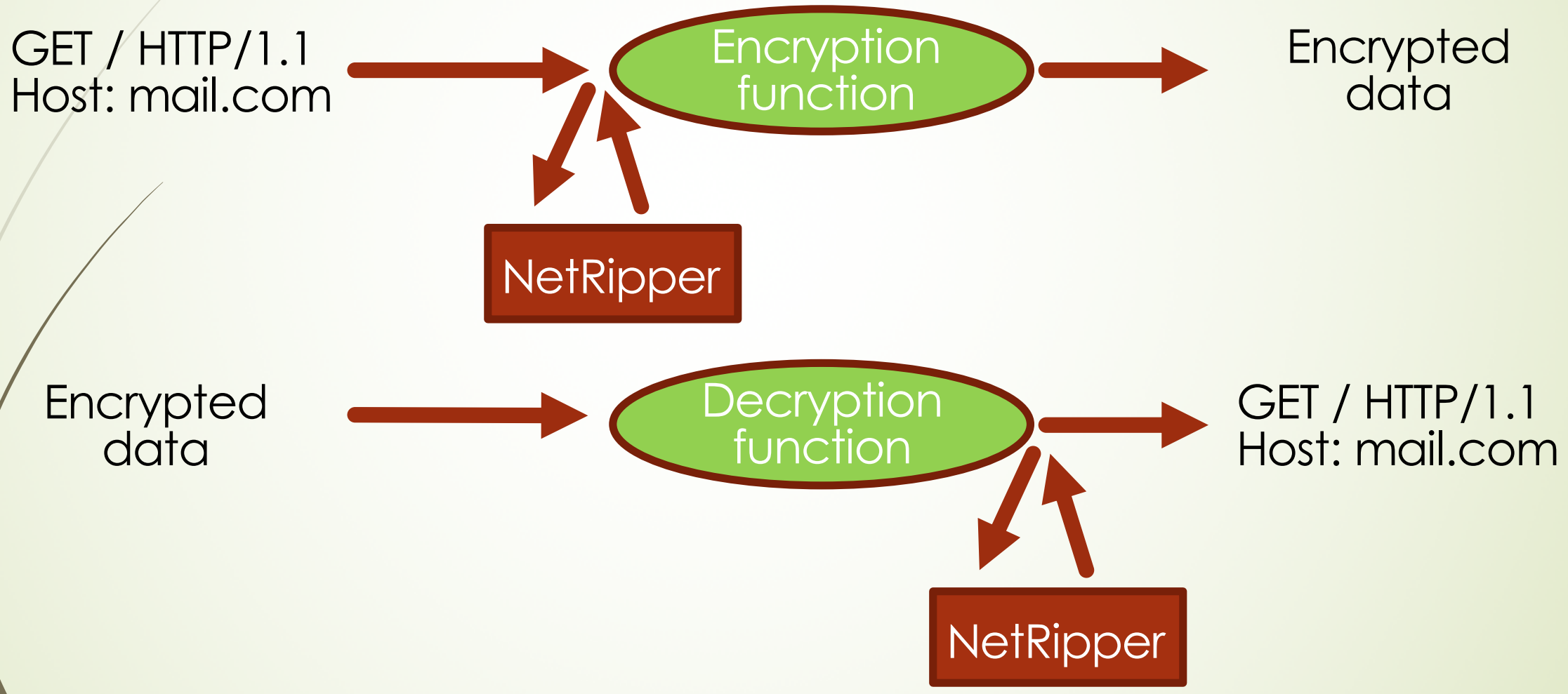
How a browser works



How NetRipper works



API Hooking


GET / HTTP/1.1
Host: mail.com
Encryption function
Encrypted data
NetRipper
Encrypted data
Decryption function
GET / HTTP/1.1
Host: mail.com
NetRipper

NetRipper components

- NetRipper.dll – Main component (API hooking)
- NetRipper.exe – DLL configurator and injector
- netripper.rb – Metasploit module of DLL configurator and injector

NetRipper plugins

- PlainText – Save only plaintext data
- DataLimit – Limit „packet” size
- StringFinder – Find strings

What's new?

- Cross-compilation on Linux
- Support for PCAP files

Cross-compilation on Linux

- Requires mingw-w64
- Compiled DLLs are big
- Has limitations
- Will be improved

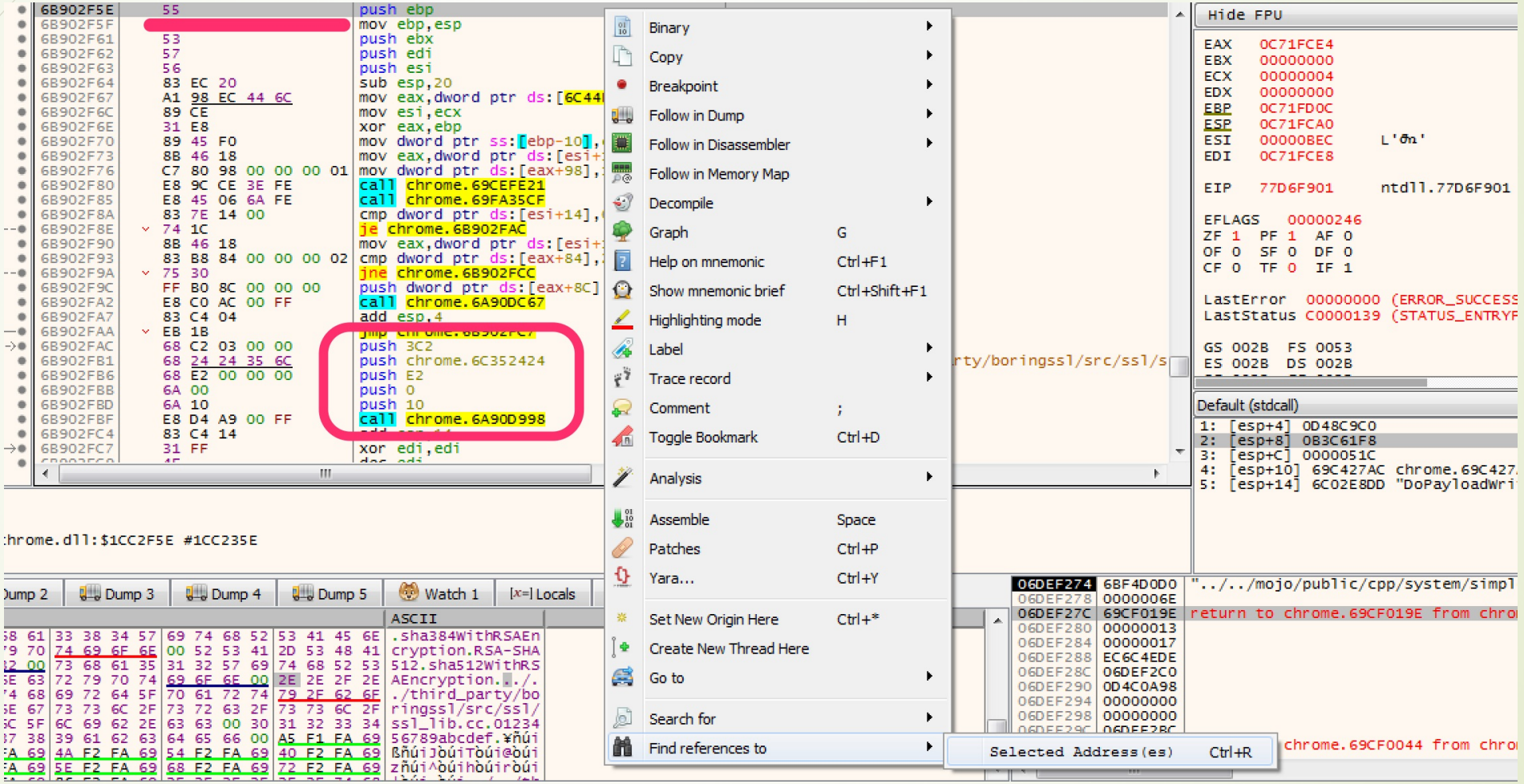
PCAP files

- Can easily follow requests and responses
- Can be used with Wireshark (supports multiple protocols)
- Can be used with other tools supporting PCAP files
- Can get IP addresses and TCP ports (limited)
- Will be improved

Where is the problem?

- Some applications are statically linked (no exported functions, reverse-engineering required)
- Support has to be added for each of them
- Examples: Putty, Google Chrome

Google Chrome



Use cases

- Penetration testers
- Bug bounty hunters
- Attackers
- Any other users

DEMO

Improvements

- Support for multiple applications
- Performance and stability
- Bypass process mitigations
- Inject in new processes
- More plugins (e.g. regular expressions)
- Support for Linux/Mac?

Conclusion

- Open-source tool for Windows
- Captures traffic before encryption and after decryption
- Supports multiple applications
- Easy to use
- It can be improved

Questions?

https://github.com/NytroRST/NetRipper

ionut.popescu@outlook.com