Protokol SFTP a FTPS

Autor: Antonín Vojtěch

Třída: 3. IT

Obsah

Obsah
Protokol SFTP a FTPS 1
Obsah 2
Co je to FTP protokol a k čemu slouží? 3
Protokol SFTP 4
Klady a zápory SFTP 5
Protokol FTPS 6
Klady a zápory FTPS 7
Praxe – Klasické FTP 8
Praxe – FTPS 12
Zdroje 14

Co je to FTP protokol a k čemu slouží?

- Je to protokol pro přenos souborů mezi počítači pomocí počítačové sítě. Využívá protokol TCP z rodiny TCP/IP a může být používán nezávisle na použitém operačním systému. Definován byl v roce 1985 v RFC 959 a rozšířen byl v roce 1997 v RFC 2228. Jeho podpora je součástí webových prohlížečů nebo tzv. FTP klientů.
- RFC je v informatice označení řady dokumentů popisujících internetové protokoly, systémy apod.

AUTHENTICATION/SECURITY MECHANISM (AUTH)

The argument field is a Telnet string identifying a supported mechanism. This string is case-insensitive. Values must be registered with the IANA, except that values beginning with "X-" are reserved for local use.

If the server does not recognize the AUTH command, it must respond with reply code 500. This is intended to encompass the large deployed base of non-security-aware ftp servers, which will respond with reply code 500 to any unrecognized command. If the server does recognize the AUTH command but does not implement the security extensions, it should respond with reply code 502.

If the server does not understand the named security mechanism, it should respond with reply code 504.

If the server is not willing to accept the named security mechanism, it should respond with reply code 534.

If the server is not able to accept the named security mechanism, such as if a required resource is unavailable, it should respond with reply code 431.

If the server is willing to accept the named security mechanism, but requires security data, it must respond with reply code 334.

If the server is willing to accept the named security mechanism, and does not require any security data, it must respond with reply code 234.

If the server is responding with a 334 reply code, it may include security data as described in the next section.

Protokol SFTP

- SFTP slouží ke stejnému účelu jako FTP, s tím rozdílem, že SFTP je zabezpečen pomocí protokolu SSH-2.
- Často lidé mylně tvrdí, že SFTP je FTP zabezpečeno pomocí protokolů SSL nebo SSH. Zabezpečit FTP pomocí SSH je možné, ale toto využití je vzácné. SFTP je zkratka pro SSH File Transfer Protocol, je to samostatný protokol.
- Oproti FTP běží na portu 22, FTP využívá porty 20 a 21 a běží výhradně přes TCP protokol. SFTP Může běžet na jakémkoliv portu, ale port 22 je nejčastější. FTP server naslouchá na portu 21 na příchozí spojení z FTP klienta. Na tomto portu běží příkazy, které zachytává server. Na portu 20 se pak přenáší pouze data. Přenos může být binární nebo ascii (textový).
- Komunikaci FTP protokolu je snadné zachytit, přečíst a zneužít (např. přihlašovací jméno, heslo i přenášená data).
- Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet.
- Nezabezpečený i zabezpečený přenos dat se dá odchytit např. pomocí programu WireShark, více o tomto tématu v prezentaci.
- Všechny příkazy (požadavky) SFTP jsou zabaleny do binárních zpráv a odeslány na server, který odpovídá binárními pakety.

Klady a zápory SFTP

- Má standardy, které přísně definují většinu (pokud ne všechny) aspekty provozu.
- Má pouze jedno připojení (není potřeba samostatné připojení pro data). Spojení je vždy zabezpečené.
- Protokol obsahuje operace pro oprávnění a manipulaci s atributy, zamykání souborů a další funkce.

- Komunikace je binární a nemůže být zaznamenána „tak, jak je“ pro lidské čtení.

- Klíče SSH je těžší spravovat a ověřovat

- Žádné operace kopírování ze serveru na server a rekurzivní odstranění adresáře.

Protokol FTPS

- Jedná se o protokol FTP který je zabezpečen pomocí protokolů SSL a TSL, jedná se o samostatné protokoly
- FTPS umožňuje šifrování příkazových i datových kanálů a ověřuje připojení pomocí kombinace ID uživatele a hesla, certifikátu nebo obou.
- Při připojení k serveru FTPS váš klient FTPS zkontroluje, zda je certifikát serveru důvěryhodný. Certifikát je považován za důvěryhodný, pokud byl: 1) podepsán známou certifikační autoritou třetí strany nebo 2) pokud byl podepsán vaším partnerem a máte kopii jejich veřejného certifikátu.
- Existují dvě metody, jak použít lze FTPS
- První metodou je Implicitní FTPS, který běží na portu 990. Pokud se klient připojí přes port 990, server předpokládá, že SSL bude vyvolán a automaticky hledá autentizační pověření. Pokud tyto nejsou k dispozici, je připojení ukončeno.
- Druhou metodou je Explicitní FTPS, která běží na portu 21. Explicitní FTPS vyžaduje, aby klient výslovně uvedl, že hodlá používat SSL. Jakmile server obdrží tento příkaz, vyhledá ověřovací pověření. Explicitní FTPS poskytuje větší flexibilitu a umožňuje klientovi dosáhnout zvýšené bezpečnosti, pokud je to nutné, nebo vyšší rychlosti, když je zabezpečení méně problematické.

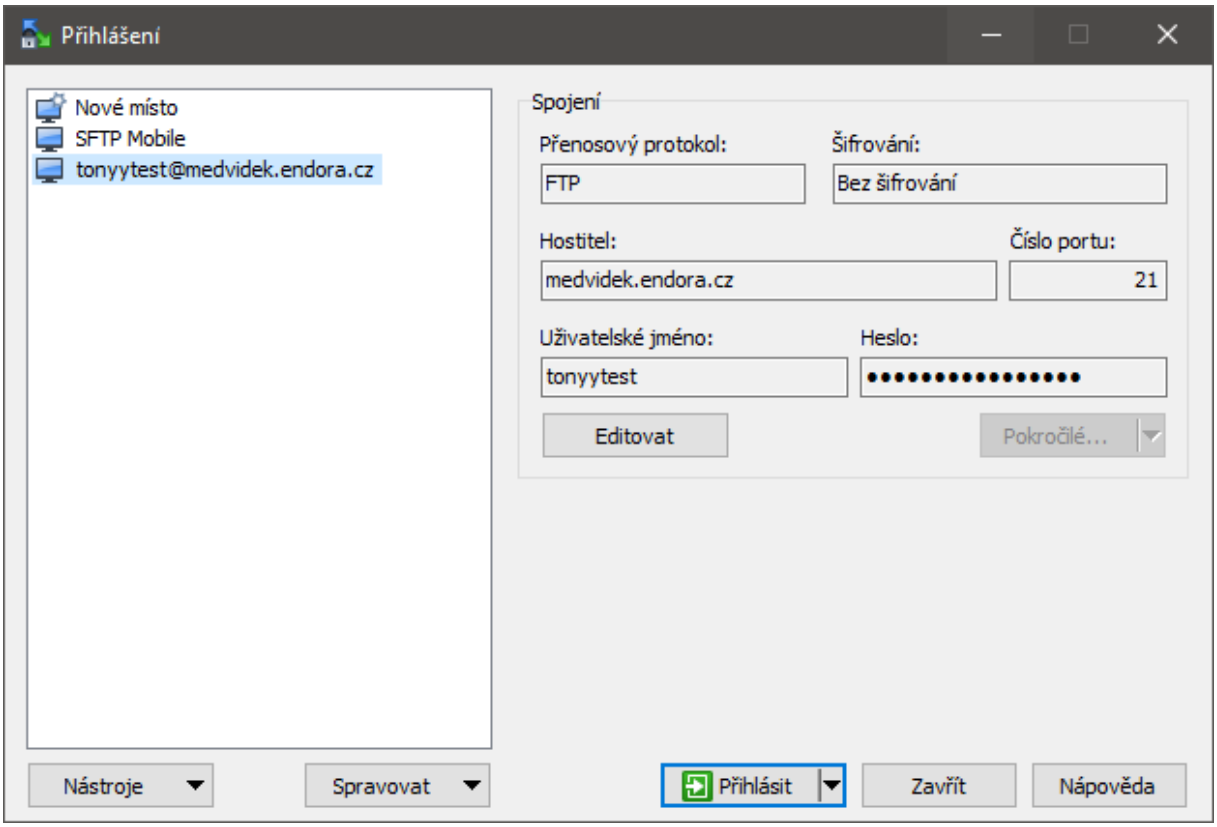
Klady a zápory FTPS

- Široce známé a používané.
- Komunikace čitelná člověkem.
- Poskytuje služby pro přenos souborů ze serveru na server.
- SSL / TLS má dobré mechanismy ověřování (funkce certifikátu X.509).
- Podpora FTP a SSL / TLS je integrována do mnoha rámců internetové komunikace.

- Vyžaduje sekundární kanál pro data, ztěžuje použití za Firewall.
- Nedefinuje standard pro znakové sady názvů souborů (kódování).
- Ne všechny FTP servery podporují SSL / TLS.
- Nemá standardní způsob, jak získat a změnit atributy souborů a adresářů.

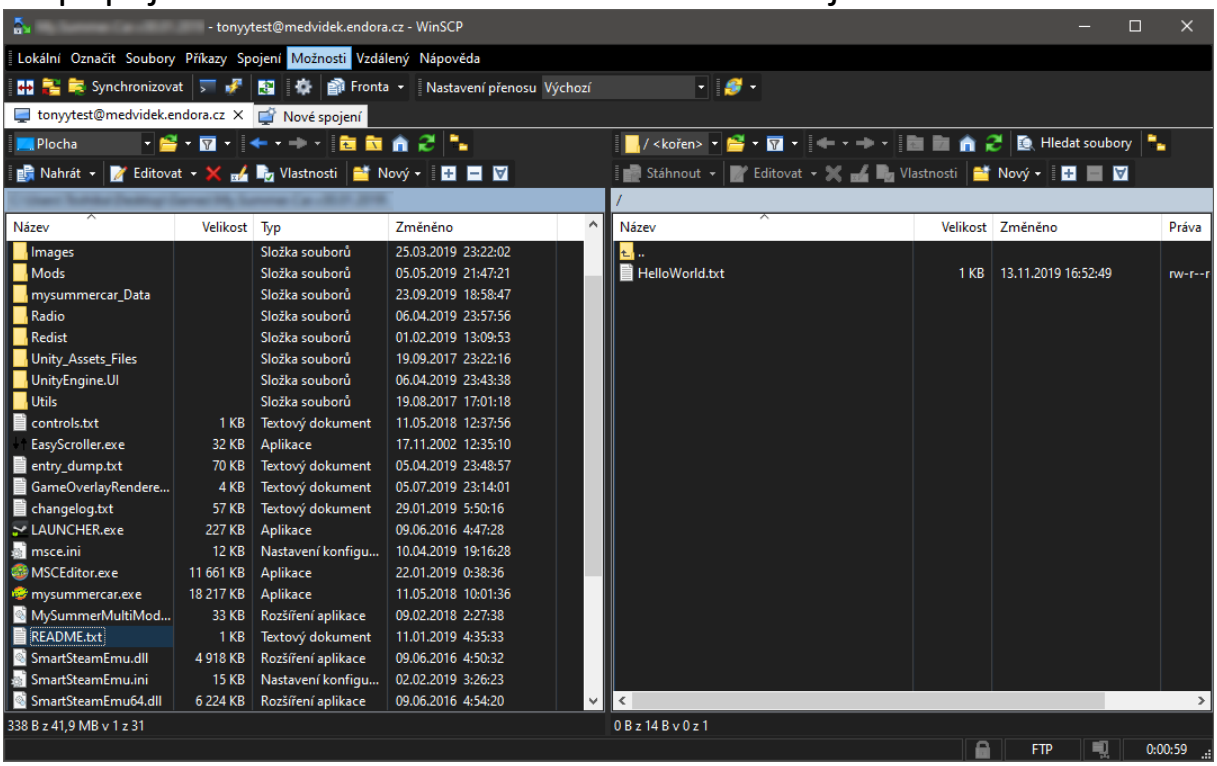
Praxe – Klasické FTP

- Pro připojení k FTP serveru jsem použil klient WinSCP, který je zdarma



- Po spuštění klienta WinSCP se zobrazí přihlašovací okénko, kde je třeba si vybrat typ připojení, hostitele a popřípadně šifrování. Dále si lze nastavit číslo portu nebo uživatelské jméno a heslo, lze se také připojit tzv. „Anonymně“ – v tomto případě se heslo zadávat nemusí.

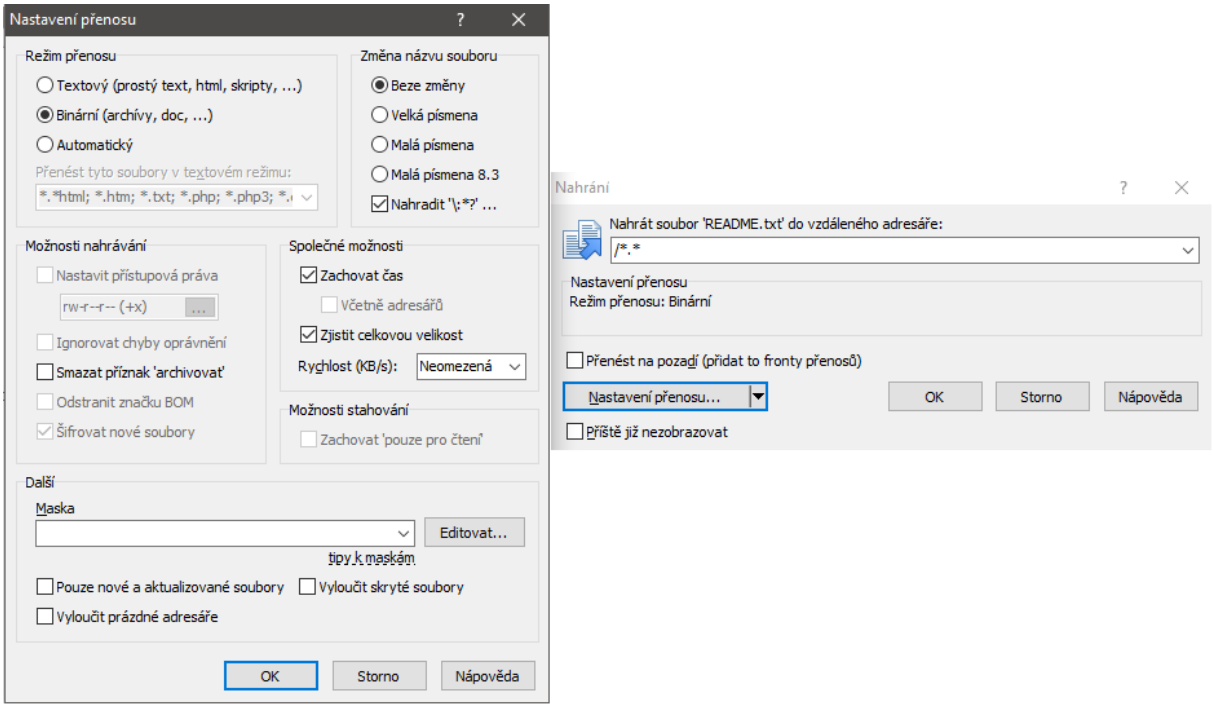
- Po připojení se na FTP server se zobrazí následující okénko



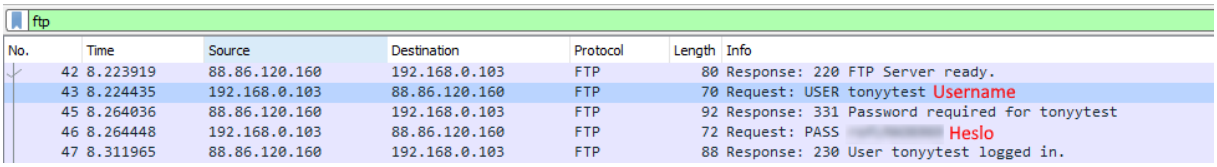
- Na levé straně se nachází adresář z počítače, na druhé se nachází adresář FTP serveru.
- Nyní si stačí vybrat jakýkoliv soubor a kliknout na tlačítko „Nahrát“

- Po kliknutí na tlačítko „Nahrát“ se zobrazí okénko, které se nachází na pravé části na následujícím obrázku. Po kliknutí na „Nastavení přenosu“ se zobrazí okénko na levé části obrázku.

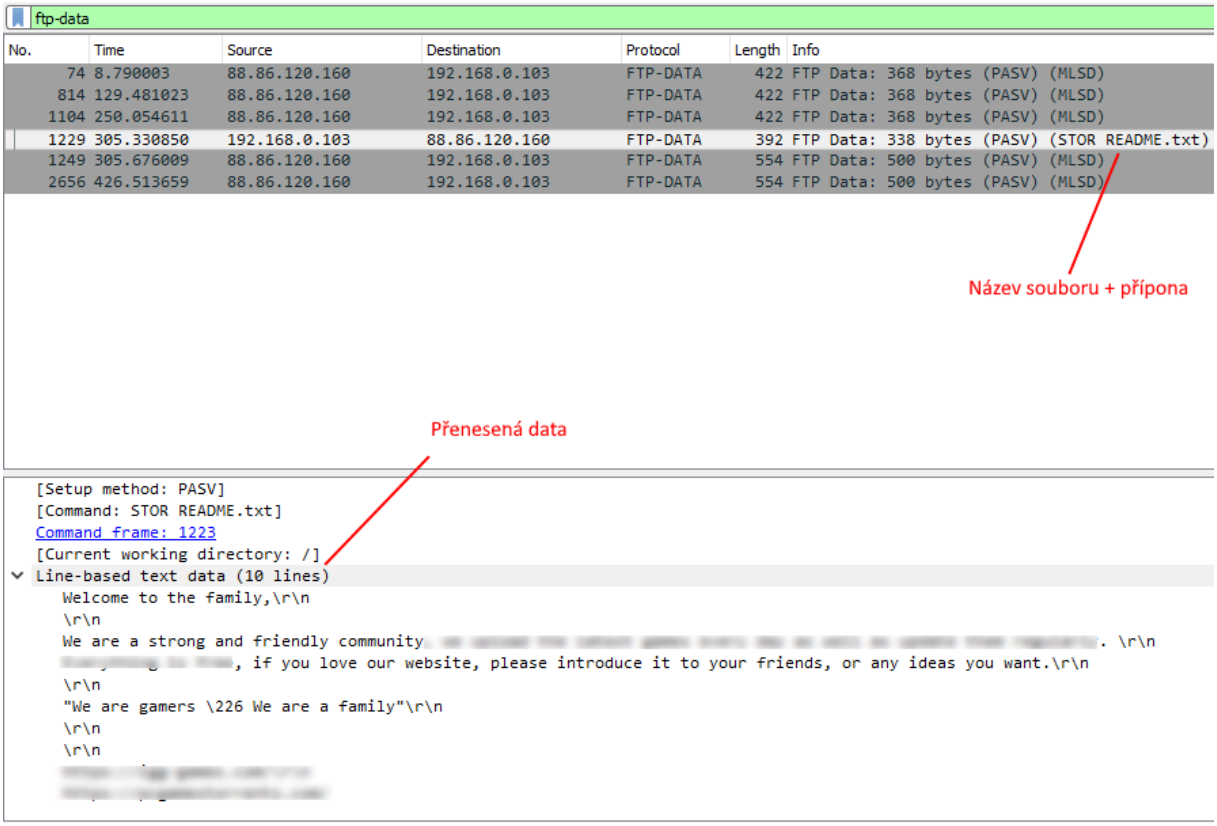
- Pokud nechcete nic nastavovat, můžete rovnou nahrát Vámi zvolený soubor.



- První část komunikace FTP klienta a serveru zahrnuje ověření přihlašovacích údajů, které jsou v nezabezpečeném FTP přenosu jednoduše odchytitelná a zneužitelná. Toto platí i pro přenášená data.
- Na následujícím obrázku je zachycena komunikace výměny přihlašovacích údajů. Jsou posílány v textové podobě.

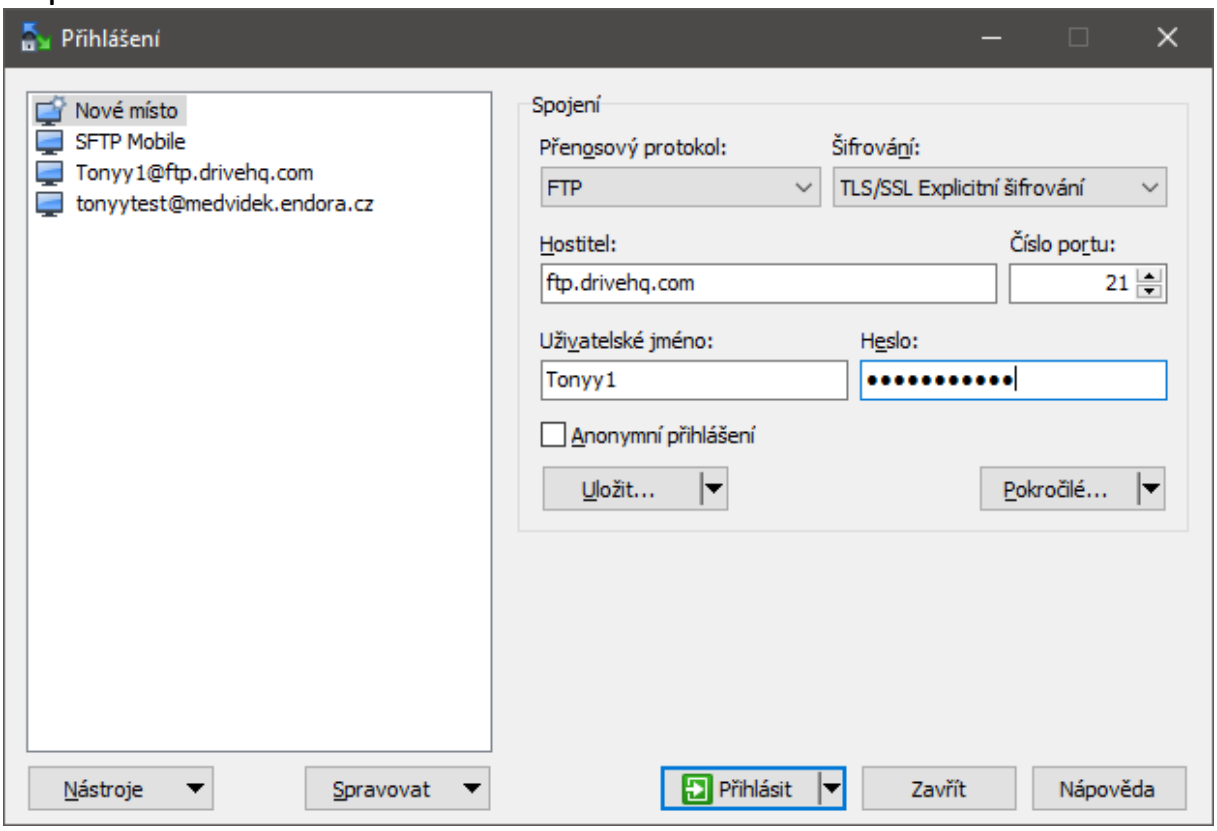


- Na následujícím obrázku je zachycena komunikace, přes kterou putovala data – tzn. Všechny přenosy souborů. Opět jsou posílány v textové podobě.

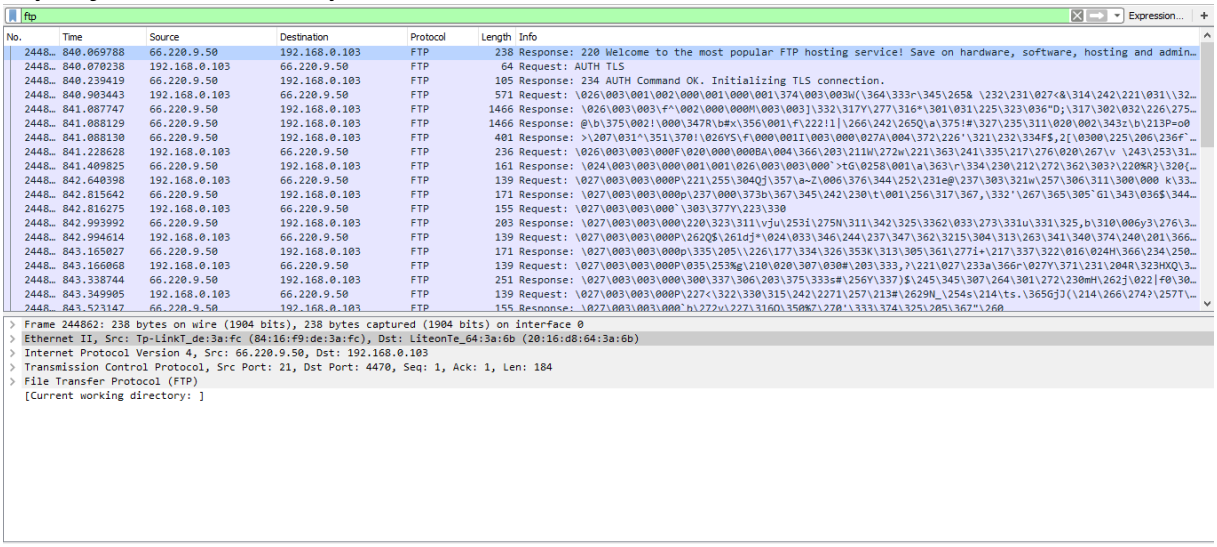


Praxe – FTPS

- Přihlašování u FTPS je téměř totožný s FTP, liší se v povinné volbě šifrování. Způsob nahrávání souborů v FTP klientovi pak zůstává totožný, rozdílný je způsob přenosů souborů a ověřování přihlašovacích údajů.
- Pro demonstraci bylo použito explicitní TLS/SSL namísto implicitního.



- Takto vypadají packety FTP šifrované přes TLS/SSL
- Nyní již nelze odchytit a zneužít FTP komunikaci



Zdroje

https://cs.wikipedia.org/wiki/FTPS
https://cs.wikipedia.org/wiki/File_Transfer_Protocol
https://cs.wikipedia.org/wiki/SSH_file_transfer_protocol
https://www.secureblackbox.com/kb/articles/FTPS-vs-SFTP.rst
https://www.thorntech.com/2019/07/ftp-ftps-sftp-differences/