МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**РОЗКРИТТЯ ПОРЯДКУ АНАЛІЗУ МЕРЕЖЕВОГО ДАМПУ, РОЗГЛЯД ПОРЯДКУ ВСТАНОВЛЕННЯ TCP СЕСІЇ**

**Виконав:** курсант 314 навчальної групи

мол. с-нт. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ І.МАРТИНЮК

**Перевiрив:** викладач кафедри № 33

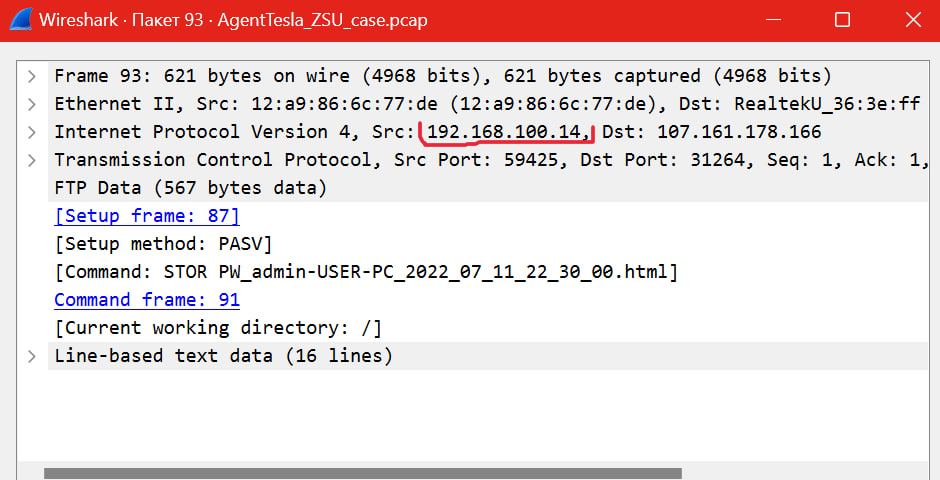
капітан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.ПРИЙМА

Київ – 2024

Було проведено аналіз кіберінциденту, що стався у військовій частині, на основі наданого файлу дампу «AgentTesla\_ZSU\_case.pcap» за допомогою програмного забезпечення Wireshark. В результаті проведеного аналізу були отримані наступні відомості про інцидент:

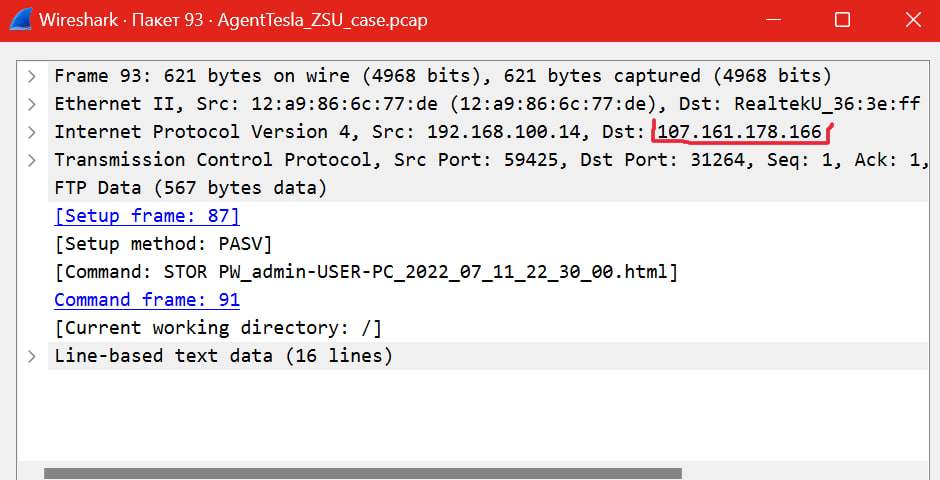
1. **IP-адреса жертви.**

***192.168.100.14***



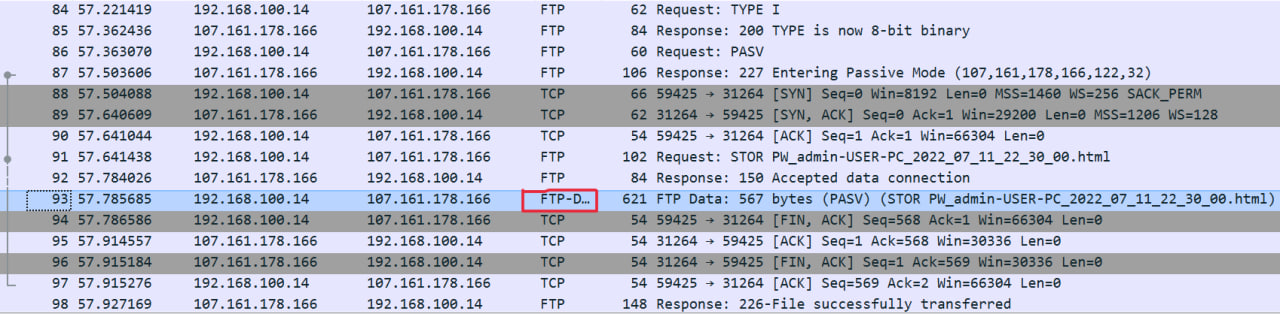
1. **IP-адреса зловмисника.**

***107.161.178.166***



1. **Протокол (канал) що використано зловмисником для ексфільтрації данних жертви.**

***FTP:***



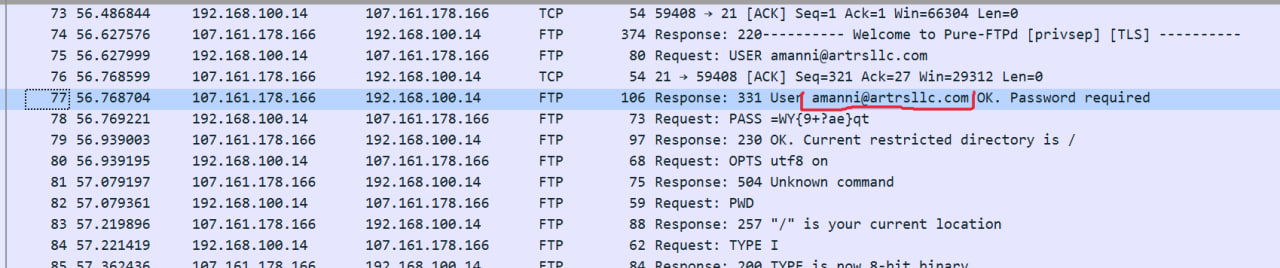
1. **Ім’я хоста жертви.**

***USER-PC:***



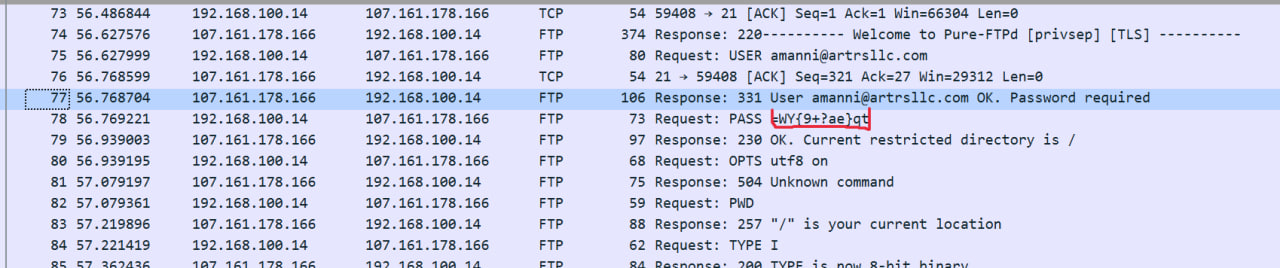
1. **Логін який використовувався зловмисником для аутентифікації на FTP-сервері.**

[***amanni@artsll.com***](mailto:amanni@artsll.com)



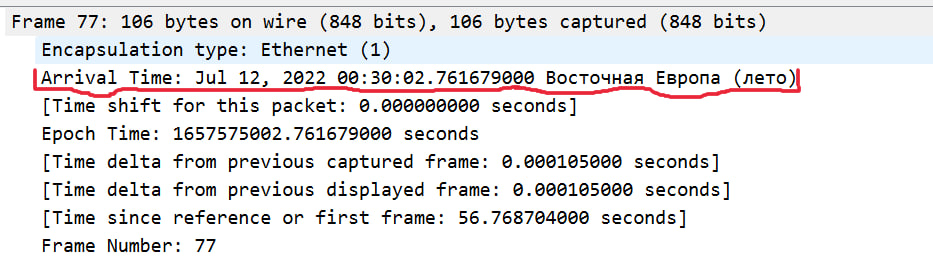
1. **Пароль який використовувався зловмисником для аутентифікації на FTP-сервері.**

***WY{9+?ae}qt***



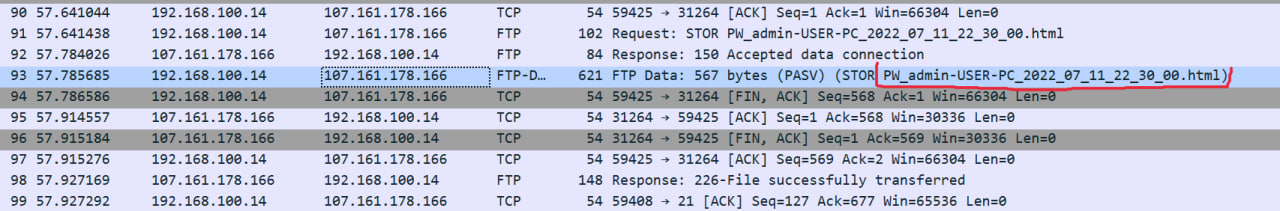
1. **Дата і час початку передачі викраденої інформації від жертви [YYYY-MM-DD HH:MM:ss]:**

***2022.07.12 00.30.03***



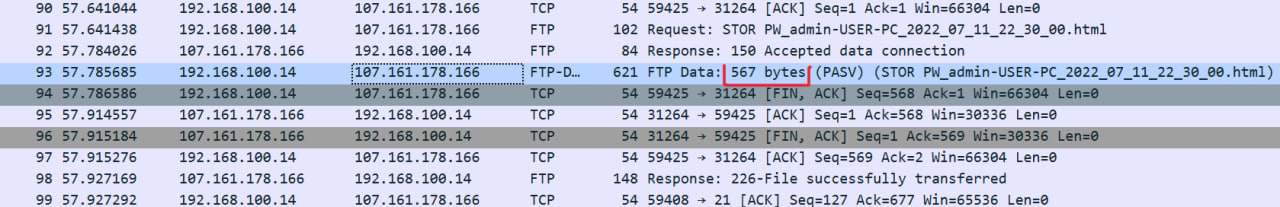
1. **Назва файлу що був завантажений з ексфільтрованими даними:**

***PW\_admin-USER-PC\_2022\_07\_11\_22\_30\_00.html***



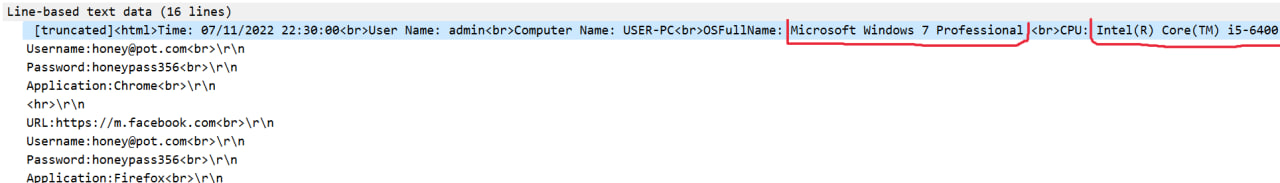
1. **Загальний об’єм інформації, що було викрадено у жертви:**

***567 bytes***



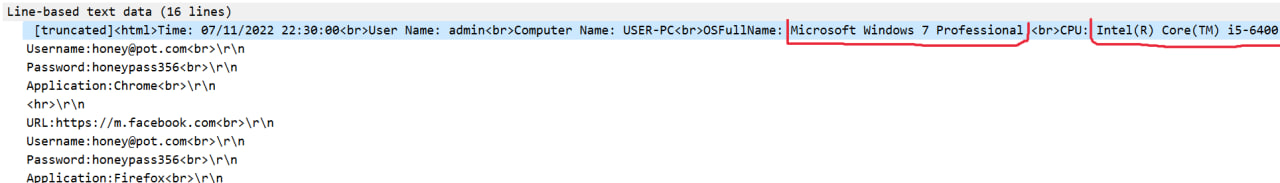
1. **Назва і версія операційної системи, що встановлена у жертви:**

***Microsoft Windows 7 Professional***



1. **Марка та модель процесора на ПК жертви:**

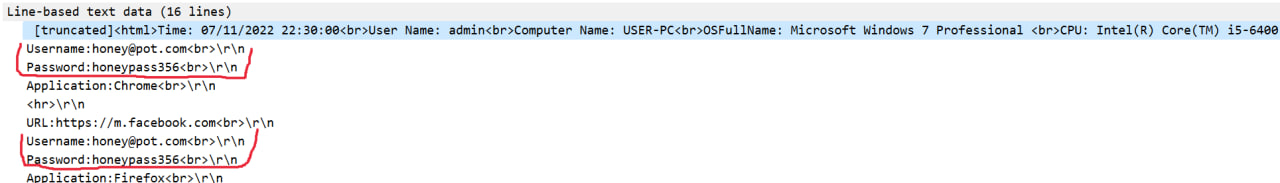
***Intel Core i5-6400***



1. **Обліковий запис жертви для поштового клієнту:**

***Username:*** [***honey@pot.com***](mailto:honey@pot.com)

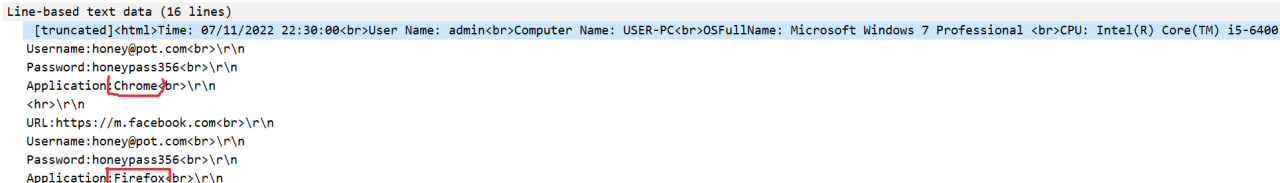
***Password: honeypass356***



1. **Браузери з яких були викрадені облікові записи жертви:**

***Chrome***

***Firefox***



**ВИСНОВОК**

Цей звіт демонструє глибокий і детальний аналіз мережевого трафіку, який був зафіксований під час кіберінциденту в військовій частині, використовуючи програмне забезпечення Wireshark. Аналіз виявив ключові аспекти інциденту, включаючи IP-адреси зловмисника та жертви, методи, за допомогою яких зловмисник здійснював несанкціонований доступ до інформації, а також специфіку використаного зловмисником протоколу для ексфільтрації даних.

Результати аналізу підкреслюють необхідність подальшого зміцнення кіберзахисту через розширення заходів безпеки та регулярне навчання персоналу для забезпечення кращого розуміння потенційних загроз і методів їх запобігання. Також це підтверджує важливість постійного моніторингу мережевих активностей для своєчасного виявлення та реагування на подібні інциденти в майбутньому.

З огляду на складність і зловмисний характер атаки, рекомендовано проводити детальний розгляд використаних кібератакантами методів та постійно оновлювати внутрішні процедури кібербезпеки для запобігання подальшим інцидентам.