Название работы

Имена

# Описание проблеммы

Многие распространённые контроллеры не поддерживают защищённое подключение инженерных программ, предназначенных для настройки и обслуживания контроллеров. Это создаёт  угрозу перехвата аутентификационных данных потенциальным нарушителем.

В ходе проведения аудита необходимо уметь обнаружить такие незащищённые соединения для последующей разработки компенсационных мер.

## Необходимый инструментарий

**Wireshark** — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.

## Исходные условия

Для проведения исследования мы получили образец информационного трафика. С помощью средств ОС мы должны совершить отправку трафика на наш компьютер и проанализировать его с помощью Wire Shark

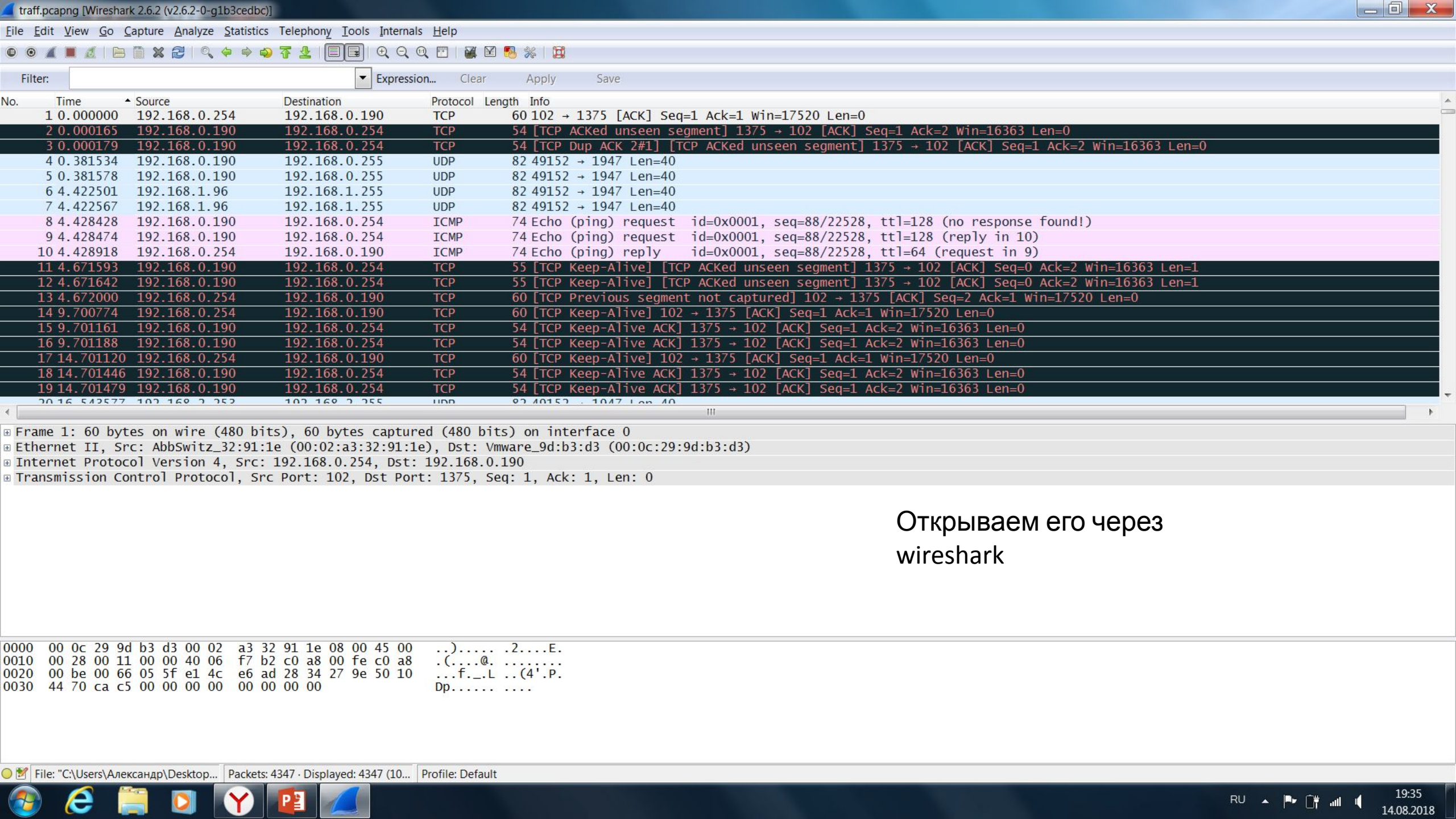
Задани
е

Обнаружить логин и пароль, с помощью которых осуществляется подключение.

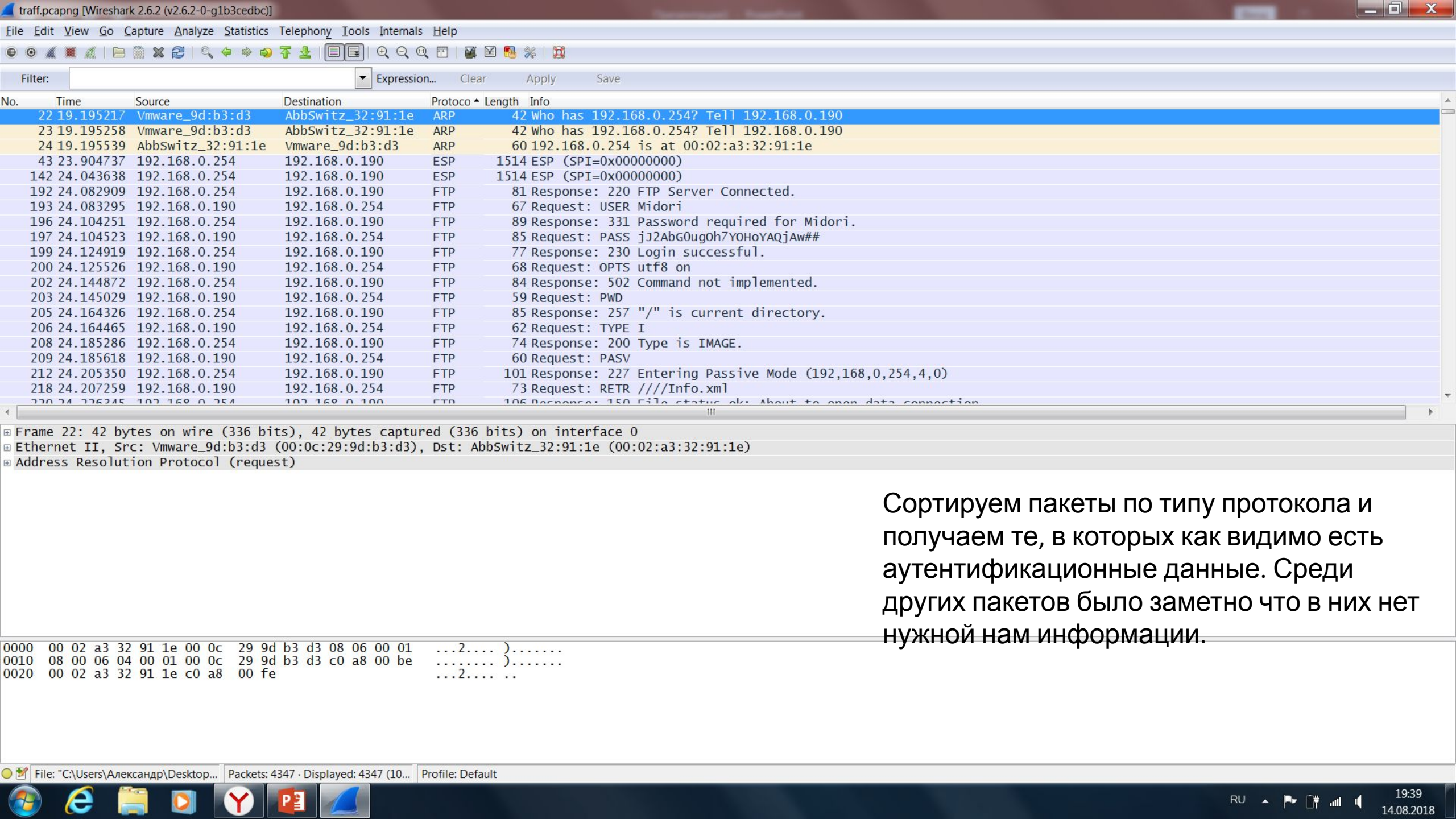
# План работы

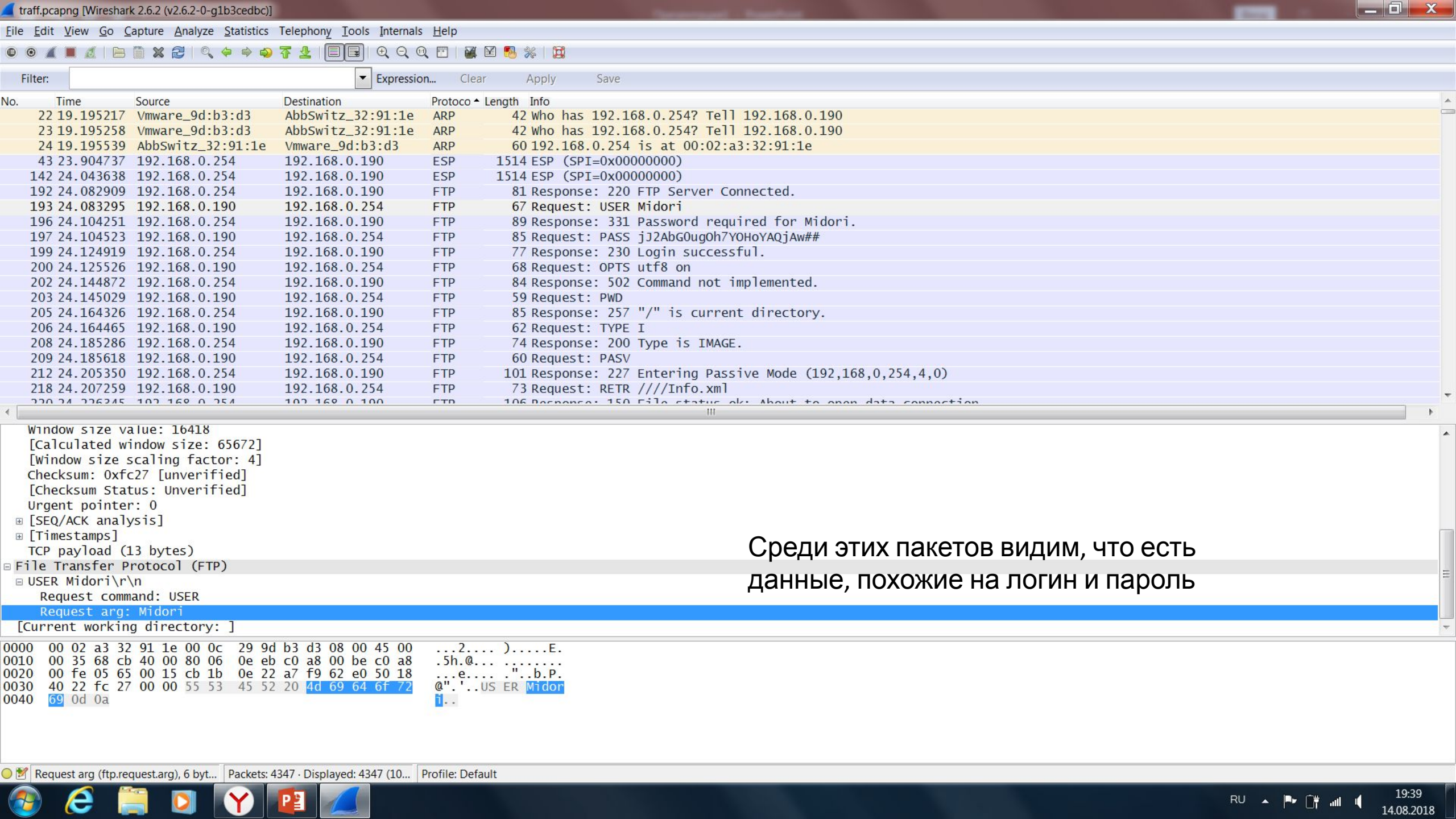
1. Получить образец трафика
2. Открыть его через wireshark
3. Найти пакеты с аутентификационными данными
4. Получить логин и пароль при помощи которых происходило подключение

# Получен готовый образец трафика

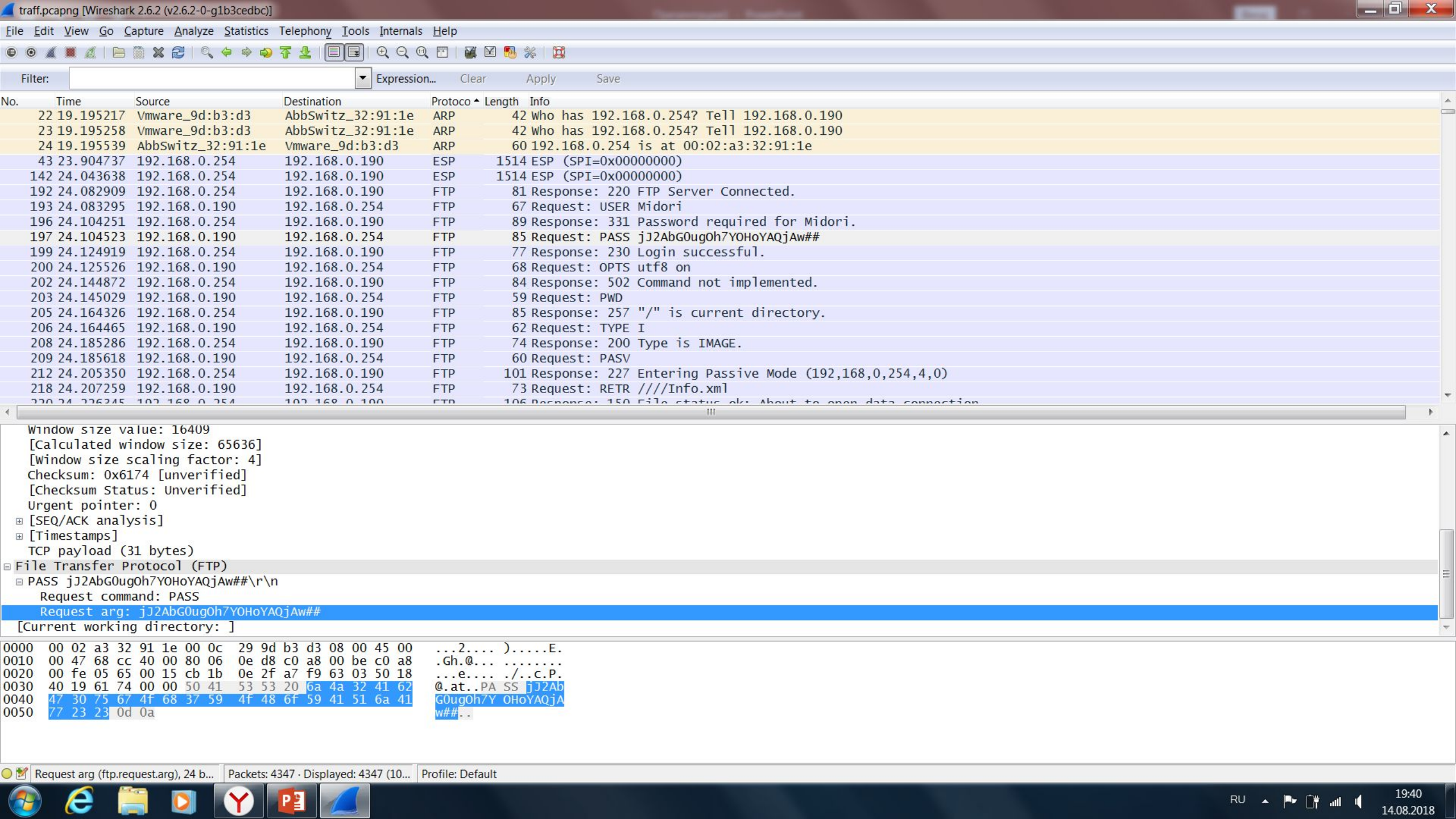



Открываем его через wireshark


traff.pcapng [Wireshark 2.6.2 (v2.6.2-0-g1b3cedbc)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protoco Length Info
22 19.195217 Vmware_9d:b3:d3 AbbSwitz_32:91:1e ARP 42 Who has 192.168.0.254? Tell 192.168.0.190
23 19.195258 Vmware_9d:b3:d3 AbbSwitz_32:91:1e ARP 42 Who has 192.168.0.254? Tell 192.168.0.190
24 19.195539 AbbSwitz_32:91:1e Vmware_9d:b3:d3 ARP 60 192.168.0.254 is at 00:02:a3:32:91:1e
43 23.904737 192.168.0.254 192.168.0.190 ESP 1514 ESP (SPI=0x00000000)
142 24.043638 192.168.0.254 192.168.0.190 ESP 1514 ESP (SPI=0x00000000)
192 24.082909 192.168.0.254 192.168.0.190 FTP 81 Response: 220 FTP Server Connected.
193 24.083295 192.168.0.190 192.168.0.254 FTP 67 Request: USER Midori
196 24.104251 192.168.0.254 192.168.0.190 FTP 89 Response: 331 Password required for Midori.
197 24.104523 192.168.0.190 192.168.0.254 FTP 85 Request: PASS jJ2AbGOugOh7YOHoYAQjAw##
199 24.124919 192.168.0.254 192.168.0.190 FTP 77 Response: 230 Login successful.
200 24.125526 192.168.0.190 192.168.0.254 FTP 68 Request: OPTS utf8 on
202 24.144872 192.168.0.254 192.168.0.190 FTP 84 Response: 502 Command not implemented.
203 24.145029 192.168.0.190 192.168.0.254 FTP 59 Request: PWD
205 24.164326 192.168.0.254 192.168.0.190 FTP 85 Response: 257 "/" is current directory.
206 24.164465 192.168.0.190 192.168.0.254 FTP 62 Request: TYPE I
208 24.185286 192.168.0.254 192.168.0.190 FTP 74 Response: 200 Type is IMAGE.
209 24.185618 192.168.0.190 192.168.0.254 FTP 60 Request: PASV
212 24.205350 192.168.0.254 192.168.0.190 FTP 101 Response: 227 Entering Passive Mode (192,168,0,254,4,0)
218 24.207259 192.168.0.190 192.168.0.254 FTP 73 Request: RETR ////Info.xml
Frame 22: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Vmware_9d:b3:d3 (00:0c:29:9d:b3:d3), Dst: AbbSwitz_32:91:1e (00:02:a3:32:91:1e)
Address Resolution Protocol (request)
0000 00 02 a3 32 91 1e 00 0c 29 9d b3 d3 08 06 00 01 ...2.... )....... 
0010 08 00 06 04 00 01 00 0c 29 9d b3 d3 c0 a8 00 be ........ )....... 
0020 00 02 a3 32 91 1e c0 a8 00 fe ...2.... ..
Сортируем пакеты по типу протокола и получаем те, в которых как видимо есть аутентификационные данные. Среди других пакетов было заметно что в них нет нужной нам информации.
File: "C:\Users\Александр\Desktop... Packets: 4347 · Displayed: 4347 (10... Profile: Default
RU 19:39 14.08.2018




Среди этих пакетов видим, что есть данные, похожие на логин и пароль


traff.pcapng [Wireshark 2.6.2 (v2.6.2-0-g1b3cedbc)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protoco Length Info
22 19.195217 Vmware_9d:b3:d3 AbbSwitz_32:91:1e ARP 42 Who has 192.168.0.254? Tell 192.168.0.190
23 19.195258 Vmware_9d:b3:d3 AbbSwitz_32:91:1e ARP 42 Who has 192.168.0.254? Tell 192.168.0.190
24 19.195539 AbbSwitz_32:91:1e Vmware_9d:b3:d3 ARP 60 192.168.0.254 is at 00:02:a3:32:91:1e
43 23.904737 192.168.0.254 192.168.0.190 ESP 1514 ESP (SPI=0x00000000)
142 24.043638 192.168.0.254 192.168.0.190 ESP 1514 ESP (SPI=0x00000000)
192 24.082909 192.168.0.254 192.168.0.190 FTP 81 Response: 220 FTP Server Connected.
193 24.083295 192.168.0.190 192.168.0.254 FTP 67 Request: USER Midori
196 24.104251 192.168.0.254 192.168.0.190 FTP 89 Response: 331 Password required for Midori.
197 24.104523 192.168.0.190 192.168.0.254 FTP 85 Request: PASS jJ2AbG0ugOh7YOHoYAQjAw##
199 24.124919 192.168.0.254 192.168.0.190 FTP 77 Response: 230 Login successful.
200 24.125526 192.168.0.190 192.168.0.254 FTP 68 Request: OPTS utf8 on
202 24.144872 192.168.0.254 192.168.0.190 FTP 84 Response: 502 Command not implemented.
203 24.145029 192.168.0.190 192.168.0.254 FTP 59 Request: PWD
205 24.164326 192.168.0.254 192.168.0.190 FTP 85 Response: 257 "/" is current directory.
206 24.164465 192.168.0.190 192.168.0.254 FTP 62 Request: TYPE I
208 24.185286 192.168.0.254 192.168.0.190 FTP 74 Response: 200 Type is IMAGE.
209 24.185618 192.168.0.190 192.168.0.254 FTP 60 Request: PASV
212 24.205350 192.168.0.254 192.168.0.190 FTP 101 Response: 227 Entering Passive Mode (192,168,0,254,4,0)
218 24.207259 192.168.0.190 192.168.0.254 FTP 73 Request: RETR ////Info.xml
Window size value: 16409
[Calculated window size: 65636]
[Window size scaling factor: 4]
Checksum: 0x6174 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[Timestamps]
TCP payload (31 bytes)
File Transfer Protocol (FTP)
PASS jJ2AbG0ugOh7YOHoYAQjAw##\r\n
Request command: PASS
Request arg: jJ2AbG0ugOh7YOHoYAQjAw##
[Current working directory: ]
0000 00 02 a3 32 91 1e 00 0c 29 9d b3 d3 08 00 45 00 ...2.... )....E.
0010 00 47 68 cc 40 00 80 06 0e d8 c0 a8 00 be c0 a8 .Gh.@... ........
0020 00 fe 05 65 00 15 cb 1b 0e 2f a7 f9 63 03 50 18 ...e.... ./..c.P.
0030 40 19 61 74 00 00 50 41 53 53 20 6a 4a 32 41 62 @.at..PA SS jJ2Ab
0040 47 30 75 67 4f 68 37 59 4f 48 6f 59 41 51 6a 41 G0ugOh7Y OHoYAQjA
0050 77 23 23 0d 0a w##..
Request arg (ftp.request.arg), 24 b...
Packets: 4347 · Displayed: 4347 (10...
Profile: Default
RU
19:40
14.08.2018

# Копируем их и получаем

Логин:
Midori

Пароль:
jJ2AbG0ugOh7YOHoYAQjAw##