

Название
работы

Имен
а

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

Задание

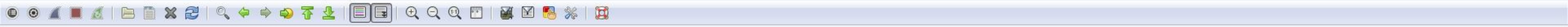
Обнаружить логин и пароль, с помощью которых осуществляется подключение.

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





Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.254	192.168.0.190	TCP	60	102 → 1375 [ACK] Seq=1 Ack=1 Win=17520 Len=0
2	0.000165	192.168.0.190	192.168.0.254	TCP	54	[TCP ACKed unseen segment] 1375 → 102 [ACK] Seq=1 Ack=2 Win=16363 Len=0
3	0.000179	192.168.0.190	192.168.0.254	TCP	54	[TCP Dup ACK 2#1] [TCP ACKed unseen segment] 1375 → 102 [ACK] Seq=1 Ack=2 Win=16363 Len=0
4	0.381534	192.168.0.190	192.168.0.255	UDP	82	49152 → 1947 Len=40
5	0.381578	192.168.0.190	192.168.0.255	UDP	82	49152 → 1947 Len=40
6	4.422501	192.168.1.96	192.168.1.255	UDP	82	49152 → 1947 Len=40
7	4.422567	192.168.1.96	192.168.1.255	UDP	82	49152 → 1947 Len=40
8	4.428428	192.168.0.190	192.168.0.254	ICMP	74	Echo (ping) request id=0x0001, seq=88/22528, ttl=128 (no response found!)
9	4.428474	192.168.0.190	192.168.0.254	ICMP	74	Echo (ping) request id=0x0001, seq=88/22528, ttl=128 (reply in 10)
10	4.428918	192.168.0.254	192.168.0.190	ICMP	74	Echo (ping) reply id=0x0001, seq=88/22528, ttl=64 (request in 9)
11	4.671593	192.168.0.190	192.168.0.254	TCP	55	[TCP Keep-Alive] [TCP ACKed unseen segment] 1375 → 102 [ACK] Seq=0 Ack=2 Win=16363 Len=1
12	4.671642	192.168.0.190	192.168.0.254	TCP	55	[TCP Keep-Alive] [TCP ACKed unseen segment] 1375 → 102 [ACK] Seq=0 Ack=2 Win=16363 Len=1
13	4.672000	192.168.0.254	192.168.0.190	TCP	60	[TCP Previous segment not captured] 102 → 1375 [ACK] Seq=2 Ack=1 Win=17520 Len=0
14	9.700774	192.168.0.254	192.168.0.190	TCP	60	[TCP Keep-Alive] 102 → 1375 [ACK] Seq=1 Ack=1 Win=17520 Len=0
15	9.701161	192.168.0.190	192.168.0.254	TCP	54	[TCP Keep-Alive ACK] 1375 → 102 [ACK] Seq=1 Ack=2 Win=16363 Len=0
16	9.701188	192.168.0.190	192.168.0.254	TCP	54	[TCP Keep-Alive ACK] 1375 → 102 [ACK] Seq=1 Ack=2 Win=16363 Len=0
17	14.701120	192.168.0.254	192.168.0.190	TCP	60	[TCP Keep-Alive] 102 → 1375 [ACK] Seq=1 Ack=1 Win=17520 Len=0
18	14.701446	192.168.0.190	192.168.0.254	TCP	54	[TCP Keep-Alive ACK] 1375 → 102 [ACK] Seq=1 Ack=2 Win=16363 Len=0
19	14.701479	192.168.0.190	192.168.0.254	TCP	54	[TCP Keep-Alive ACK] 1375 → 102 [ACK] Seq=1 Ack=2 Win=16363 Len=0

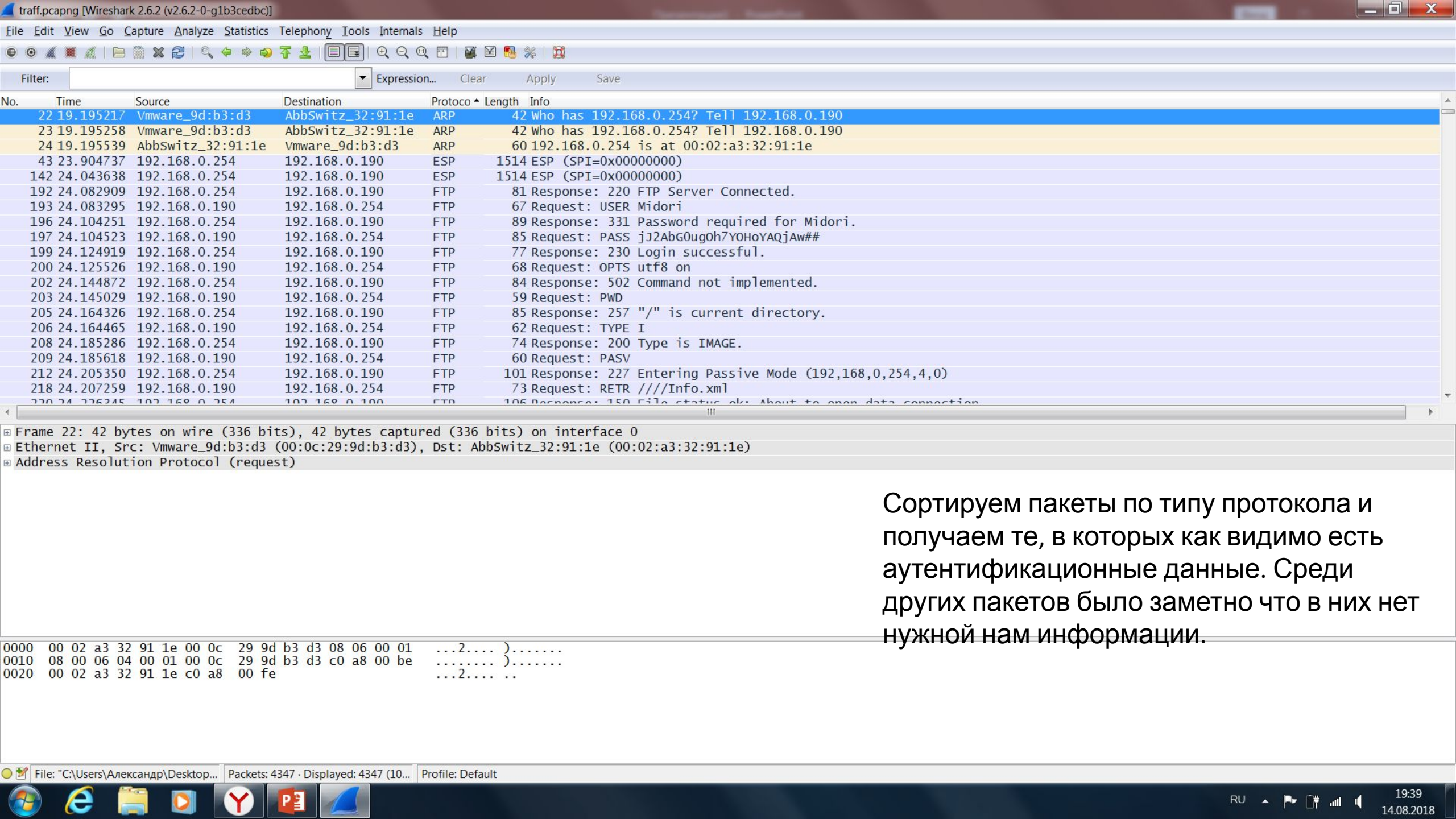
- Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: AbbSwitz_32:91:1e (00:02:a3:32:91:1e), Dst: Vmware_9d:b3:d3 (00:0c:29:9d:b3:d3)
- Internet Protocol Version 4, Src: 192.168.0.254, Dst: 192.168.0.190
- Transmission Control Protocol, Src Port: 102, Dst Port: 1375, Seq: 1, Ack: 1, Len: 0

Открываем его через wireshark

```

0000  00 0c 29 9d b3 d3 00 02  a3 32 91 1e 08 00 45 00  ..). .... .2....E.
0010  00 28 00 11 00 00 40 06  f7 b2 c0 a8 00 fe c0 a8  .(. ....@. ....
0020  00 be 00 66 05 5f e1 4c  e6 ad 28 34 27 9e 50 10  ...f...L ..(4'.P.
0030  44 70 ca c5 00 00 00 00  00 00 00 00

```

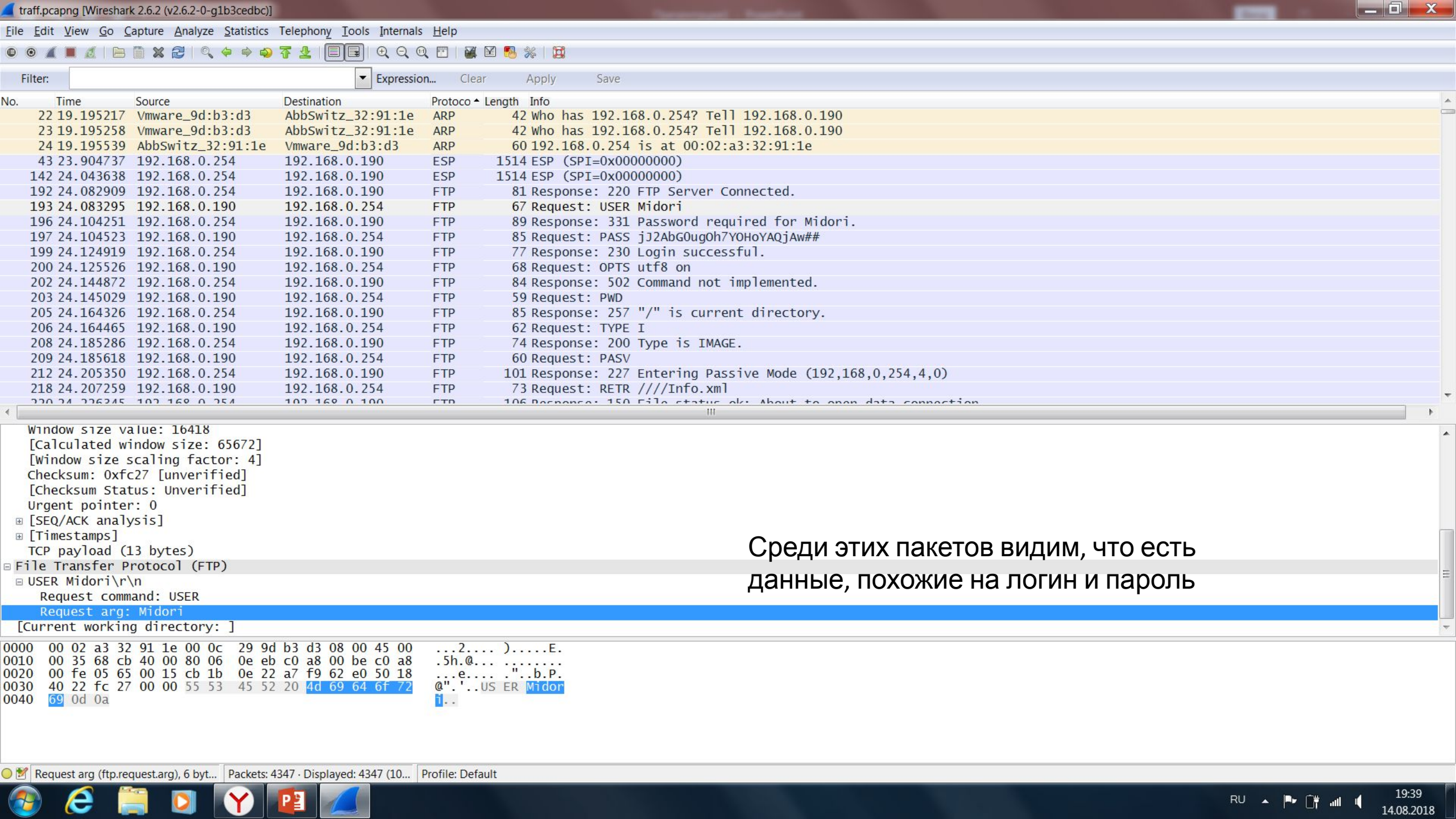


No.	Time	Source	Destination	Protocol	Length	Info
22	19.195217	Vmware_9d:b3:d3	AbbSwitz_32:91:1e	ARP	42	Who has 192.168.0.254? Tell 192.168.0.190
23	19.195258	Vmware_9d:b3:d3	AbbSwitz_32:91:1e	ARP	42	Who has 192.168.0.254? Tell 192.168.0.190
24	19.195539	AbbSwitz_32:91:1e	Vmware_9d:b3:d3	ARP	60	192.168.0.254 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 jj2AbG0ugOh7Y0HoYAQjAw##
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
220	24.226245	192.168.0.254	192.168.0.190	FTP	106	Response: 150 File status ok; About to open data connection

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)

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.

```
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.... ..
```

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



Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	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 jj2AbG0ug0h7Y0HoYAQjAw##
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
220	24.226245	192.168.0.254	192.168.0.190	FTP	106	Response: 150 File status ok; About to open data connection

```

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)
  Request command: PASS
  Request arg: jj2AbG0ug0h7Y0HoYAQjAw##
[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	G0ug0h7Y 0HoYAQjA
0050	77 23 23 0d 0a	w##..

Копируем их и
получаем

Логин:

Маркер:

jJ2AbG0ugOh7Y0HoYAQjAw##