Министерство науки и высшего образования Российской Федерации
Брянский государственный технический университет

Практическая работа №3
для слушателей программы повышения квалификации
«Основы компьютерной криминалистики
и методики реагирования на инциденты информационной
безопасности»

Брянск
БГТУ
2022

Брянский государственный технический университет
241035, Брянск, бульвар 50 лет Октября, 7.
Кафедра «Системы информационной безопасности», тел. 58-82-16.

Заполнить протокол, используя программы лекции 3
ПРОТОКОЛ № 2 от 2021 г.

Комиссия в составе:

Начала осмотр в:

Осмотр окончен:

Особенности осмотра:

Описание конфигурации устройств и программного обеспечения компьютера:

Объект осмотра:

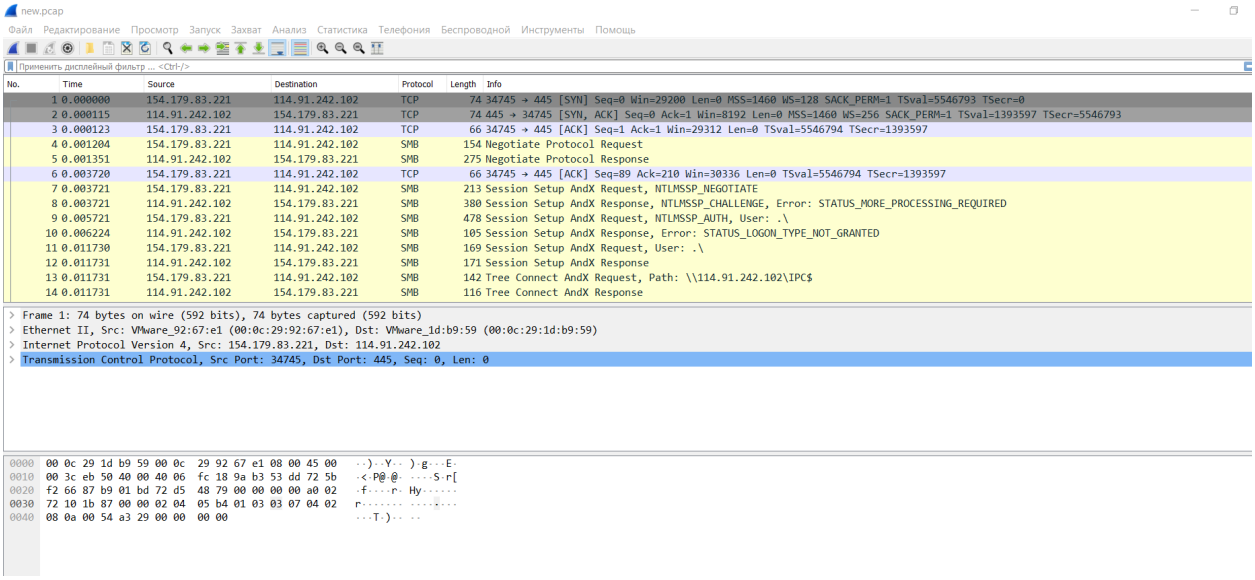
Имя компьютера, на котором проводится осмотр: оперативная **память**:

Программы участвующие в анализе сетевого дампа:

Перед комиссией поставлены следующие вопросы:

1. Является ли представленный дамп работоспособным?

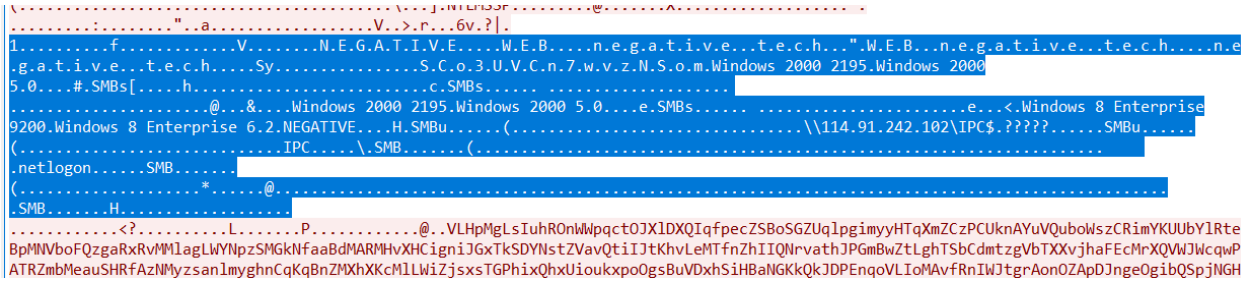
Да, является



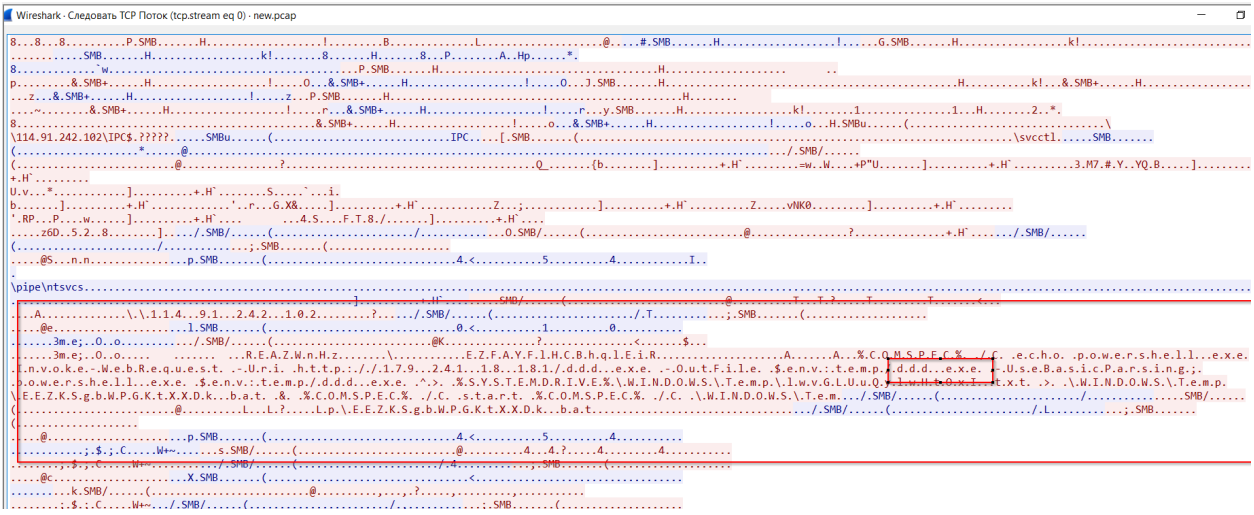
2. Присутствуют ли в сетевом дампе вредоносные программы, т.е. приводящие к несанкционированному уничтожению, блокированию, модификации, копированию информации с носителей ПЭВМ без предварительного уведомления об этих операциях собственника компьютерной информации?

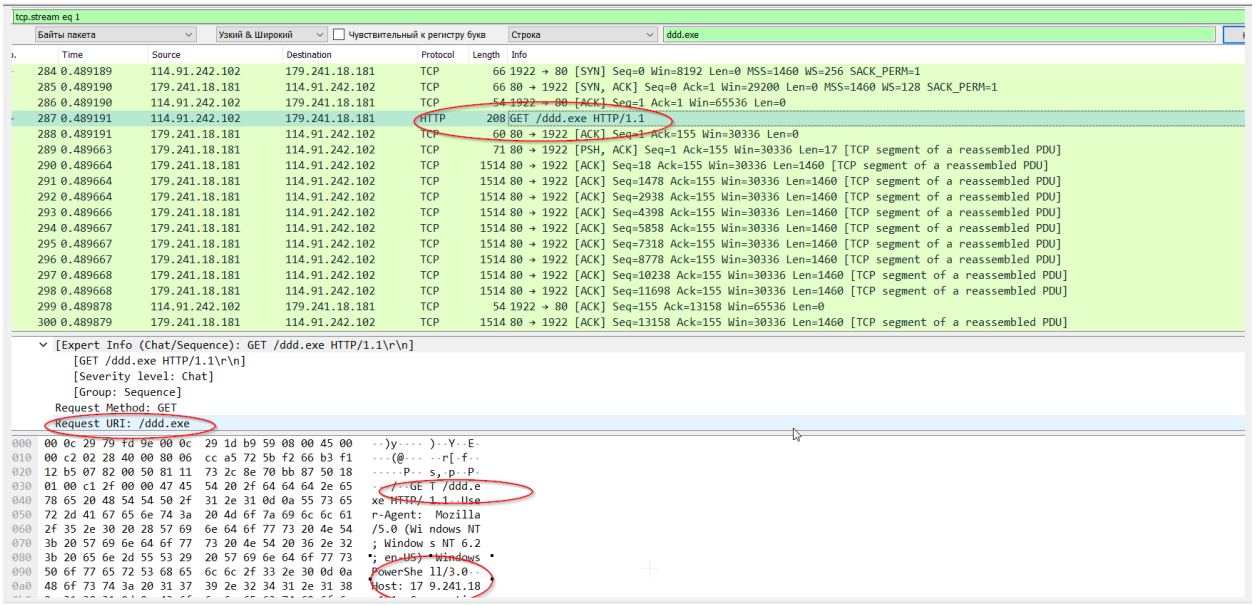
Да, присутствуют. Вирусный файл ddd.exe, который запускался через powershell

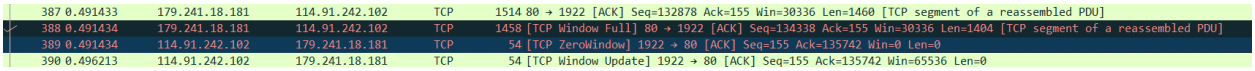
Отправка пакетов на адрес 114.91.242.102



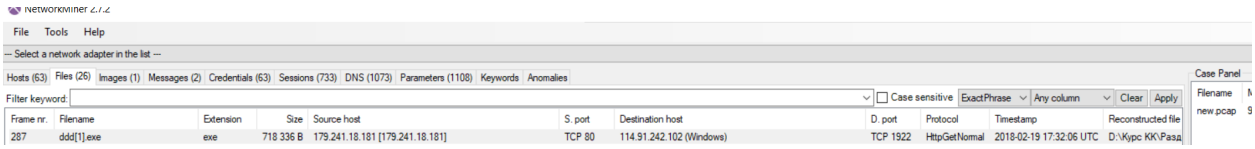
Запуск файла ddd.exe







387	0.491433	179.241.18.181	114.91.242.102	TCP	1514 80 → 1922 [ACK] Seq=132878 Ack=155 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
388	0.491434	179.241.18.181	114.91.242.102	TCP	1458 [TCP Window Full] 80 → 1922 [ACK] Seq=134338 Ack=155 Win=30336 Len=1404 [TCP segment of a reassembled PDU]
389	0.491434	114.91.242.102	179.241.18.181	TCP	54 [TCP ZeroWindow] 1922 → 80 [ACK] Seq=155 Ack=135742 Win=0 Len=0
390	0.496213	114.91.242.102	179.241.18.181	TCP	54 [TCP Window Update] 1922 → 80 [ACK] Seq=155 Ack=135742 Win=65536 Len=0



NetworkMiner 2.7.2

File Tools Help

-- Select a network adapter in the list --

Hosts (63) Files (26) Images (1) Messages (2) Credentials (63) Sessions (733) DNS (1073) Parameters (1108) Keywords Anomalies

Filter keyword: Case sensitive ExactPhrase Any column Clear Apply

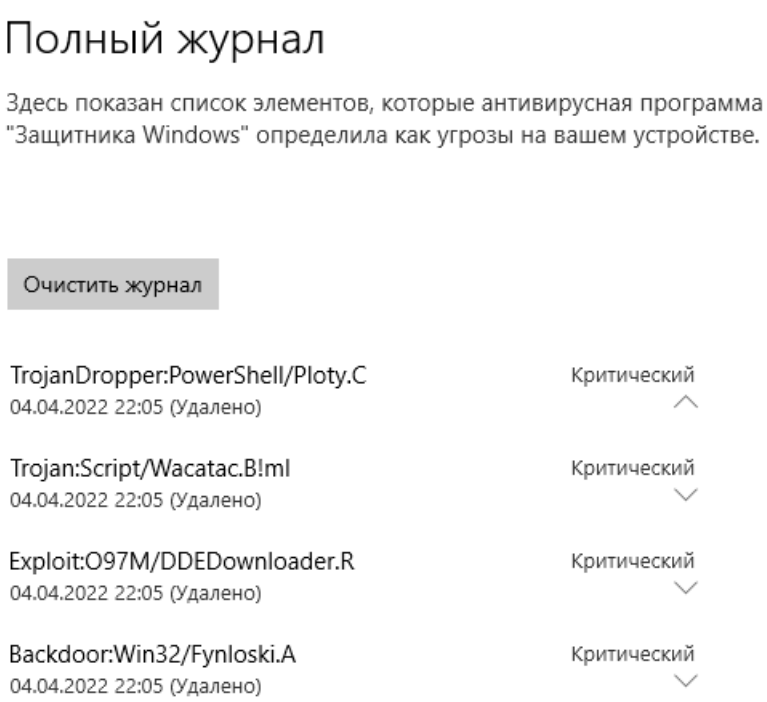
Case Panel

Filename

new.pcap

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp	Reconstructed file
287	ddd[1].exe	exe	718 336 B	179.241.18.181 [179.241.18.181]	TCP 80	114.91.242.102 (Windows)	TCP 1922	HttpGetNormal	2018-02-19 17:32:06 UTC	D:\Курс КК\Разд

+файлы удалены антивирусом при запуске networkminer



Полный журнал

Здесь показан список элементов, которые антивирусная программа "Защитника Windows" определила как угрозы на вашем устройстве.

Очистить журнал

TrojanDropper:PowerShell/Ploty.C — Критический
04.04.2022 22:05 (Удалено)

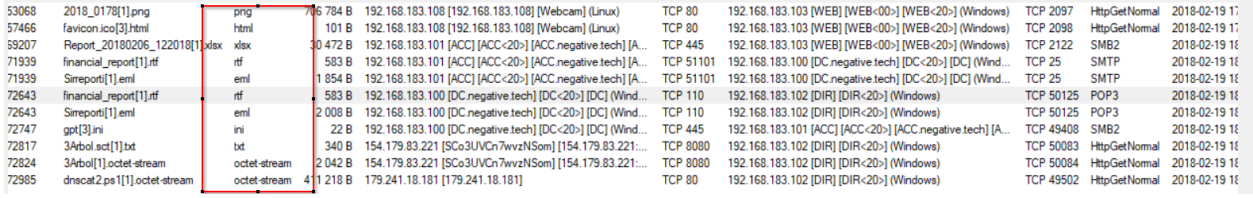
Trojan:Script/Wacatac.B!ml — Критический
04.04.2022 22:05 (Удалено)

Exploit:O97M/DDEDownloader.R — Критический
04.04.2022 22:05 (Удалено)

Backdoor:Win32/Fynloski.A — Критический
04.04.2022 22:05 (Удалено)

3. Содержат ли какие-то процессы подозрительные расположения файлов?

Да, во всех этих процессах антивирус находит зараженные файлы:



53068	2018_0178[1].png	png	706 784 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2097	HttpGetNormal	2018-02-19 17
57466	favicon.ico[3].html	html	101 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2098	HttpGetNormal	2018-02-19 17
59207	Report_20180206_122018[1].xlsx	xlsx	30 472 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 445	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2122	SMB2	2018-02-19 18
71939	financial_report[1].rtf	rtf	583 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 51101	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 25	SMTP	2018-02-19 18
71939	Sireporti[1].eml	eml	1 854 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 51101	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 25	SMTP	2018-02-19 18
72643	financial_report[1].rtf	rtf	583 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 110	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50125	POP3	2018-02-19 18
72643	Sireporti[1].eml	eml	2 008 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 110	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50125	POP3	2018-02-19 18
72747	gpt[3].ini	ini	22 B	192.168.183.100 [DC.negative.tech] [DC<20>] [DC] (Wind...	TCP 445	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 49408	SMB2	2018-02-19 18
72817	3Arbol.sct[1].txt	txt	340 B	154.179.83.221 [SCo3UVCn7wvzNSom] [154.179.83.221:...	TCP 8080	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50083	HttpGetNormal	2018-02-19 18
72824	3Arbol[1].octet-stream	octet-stream	2 042 B	154.179.83.221 [SCo3UVCn7wvzNSom] [154.179.83.221:...	TCP 8080	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 50084	HttpGetNormal	2018-02-19 18
72985	dnscat2.ps1[1].octet-stream	octet-stream	411 218 B	179.241.18.181 [179.241.18.181]	TCP 80	192.168.183.102 [DIR] [DIR<20>] (Windows)	TCP 49502	HttpGetNormal	2018-02-19 18

Например, dnscat2.ps – бэкдор для dns-туннеля

4. Возможно ли установить хронологию событий до утечки информации, возможно ли ее описать?

Злоумышленник проводил сканирование портов

Wireshark · Conversations · new.pcap

Ethernet · 27 | IPv4 · 25 | IPv6 · 4 | TCP · 787 | UDP · 1123

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B
192.168.183.103	1994	192.168.183.101	139	24	3490	13	1681	11	1809	003.45621	12.0393	1117	
192.168.183.103	57627	192.168.183.108	587	2	118	1	58	1	60	016.36920	0.0000	—	
192.168.183.102	49488	192.168.183.100	445	28	7257	16	4835	12	2422	026.31669	12.0249	3216	
192.168.183.103	40634	192.168.183.101	80	2	112	1	58	1	54	107.94075	0.0000	—	
192.168.183.103	40634	192.168.183.102	80	2	112	1	58	1	54	107.94075	0.0000	—	
192.168.183.103	40634	192.168.183.108	80	3	172	2	112	1	60	107.94075	0.0000	—	
192.168.183.103	40634	192.168.183.254	80	1	58	1	58	0	0	107.94075	0.0000	—	
192.168.183.103	40634	192.168.183.100	80	2	112	1	58	1	54	107.94075	0.0000	—	
192.168.183.103	40634	192.168.183.101	1723	2	112	1	58	1	54	107.94078	0.0000	—	
192.168.183.103	40634	192.168.183.102	1723	2	112	1	58	1	54	107.94078	0.0000	—	
192.168.183.103	40634	192.168.183.108	1723	2	118	1	58	1	60	107.94078	0.0000	—	
192.168.183.103	40634	192.168.183.254	1723	1	58	1	58	0	0	107.94078	0.0000	—	
192.168.183.103	40634	192.168.183.100	1723	2	112	1	58	1	54	107.94079	0.0000	—	
192.168.183.103	40634	192.168.183.108	995	2	118	1	58	1	60	107.95735	0.0000	—	
192.168.183.103	40634	192.168.183.254	995	1	58	1	58	0	0	107.95735	0.0000	—	
192.168.183.103	40634	192.168.183.100	995	2	112	1	58	1	54	107.95735	0.0000	—	
192.168.183.103	40634	192.168.183.101	995	2	112	1	58	1	54	107.95735	0.0000	—	
192.168.183.103	40634	192.168.183.102	995	2	112	1	58	1	54	107.95735	0.0005	—	
192.168.183.103	40634	192.168.183.108	445	3	172	2	112	1	60	107.95735	0.0006	—	
192.168.183.103	40634	192.168.183.254	445	1	58	1	58	0	0	107.95735	0.0000	—	
192.168.183.103	40634	192.168.183.100	445	3	170	2	112	1	58	107.95792	0.0000	—	
192.168.183.103	40634	192.168.183.101	445	3	170	2	112	1	58	107.95792	0.0000	—	
192.168.183.103	40634	192.168.183.102	445	3	170	2	112	1	58	107.95792	0.0000	—	
192.168.183.103	40634	192.168.183.108	587	2	118	1	58	1	60	107.95792	0.0000	—	
192.168.183.103	40634	192.168.183.254	587	1	58	1	58	0	0	107.95794	0.0000	—	

Злоумышленник начиная с 19.02.2018 17:52:19 проводит подбор пароля на компьютере с linux 192.168.183.108

192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	root	root	Unknown	2018-02-19 17:52:19 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	admin	admin	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	administrator	administrator	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	webadmin	webadmin	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	sysadmin	sysadmin	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	netadmin	netadmin	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	guest	guest	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	user	user	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	web	web	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	test	test	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	root		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	admin		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	administrator		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	webadmin		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	sysadmin		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	netadmin		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	guest		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	user		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	web		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	test		Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	root	123456	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	admin	123456	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	administrator	123456	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	webadmin	123456	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	sysadmin	123456	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	netadmin	123456	Unknown	2018-02-19 17:53:41 UTC
192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	HTTP	guest	123456	Unknown	2018-02-19 17:53:41 UTC

Далее 19.02.2018 17:54:45 с 192.168.183.108 был загружен файл – картинка, формат .png

52593	favicon.ico[2].html	html	101 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2096	HttpGetNormal	2018-0
53068	2018_0178[1].png	png	706 784 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2097	HttpGetNormal	2018-0
57466	favicon.ico[3].html	html	101 B	192.168.183.108 [192.168.183.108] [Webcam] (Linux)	TCP 80	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2098	HttpGetNormal	2018-0
69207	Report_20180206_122018[1].xlsx	xlsx	30 472 B	192.168.183.101 [ACC] [ACC<20>] [ACC.negative.tech] [A...	TCP 445	192.168.183.103 [WEB] [WEB<00>] [WEB<20>] (Windows)	TCP 2122	SMB2	2018-0

В картинке был сохранен пароль от системы авторизации-аутентификации,

File Tools Help

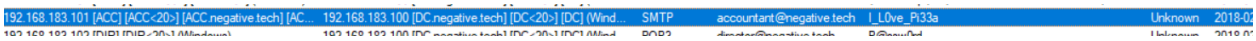
-- Select a network adapter in the list --

Hosts (63) | Files (26) | Images (1) | Messages (2) | Credentials (63) | Sessions (733) | DNS (1073) | Parameters (1108) | Keywords | Anomalies

2018_0178[1].png
3024x3024, 706 784 B

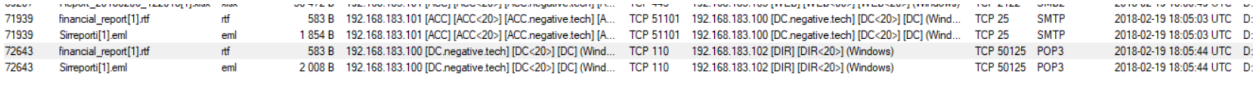
Так как далее злоумышленник 19.02.2018 17:55:54 взаимодействует с Kerberos, получая доступы к компьютерам 192.168.183.100, 192.168.183.101, 192.168.183.103

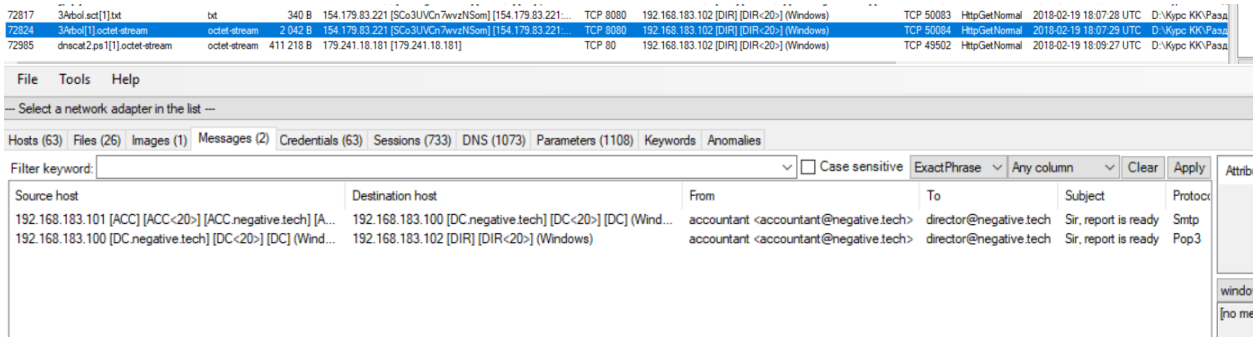
И после к компьютеру бухгалтера



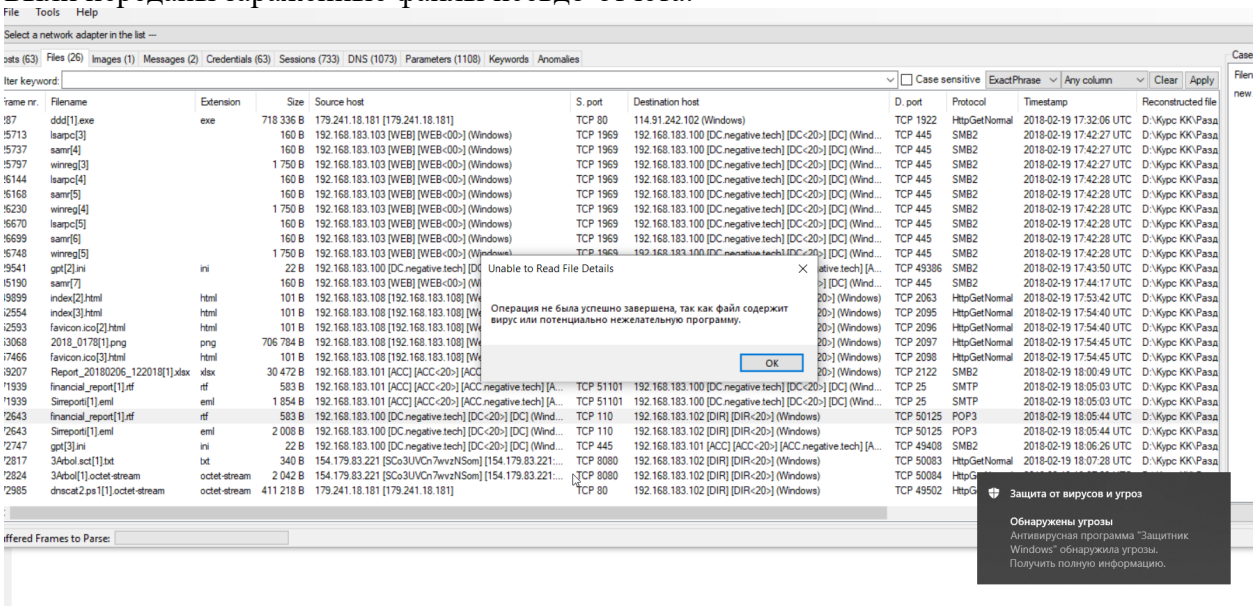
5. Как злоумышленник проник на компьютер директора?

С компьютера бухг был отправлен зараженный email на компьютер директора 192.168.183.102





Были переданы зараженные файлы псевдо-отчета:



Через зараженный отчет был получен доступ к компьютеру директора

В момент осмотра установлены:

Результаты осмотра:

Комиссия постановила:

Подписи членов комиссии: