ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Санкт-Петербургский государственный университет телекоммуникаций

им. проф. М.А. Бонч-Бруевича***»***

(СПБГУТ)

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

Факультет ИКСС

Кафедра ЗСС

Отчет по лабораторной работе №10

по дисциплине:

**«Цифровая криминалистика»**

Выполнили:

Студенты гр. ИКТБ-98м

Зеличенок И.Ю.

Щипцов Д.И.

Проверила:

Федорченко Е.В

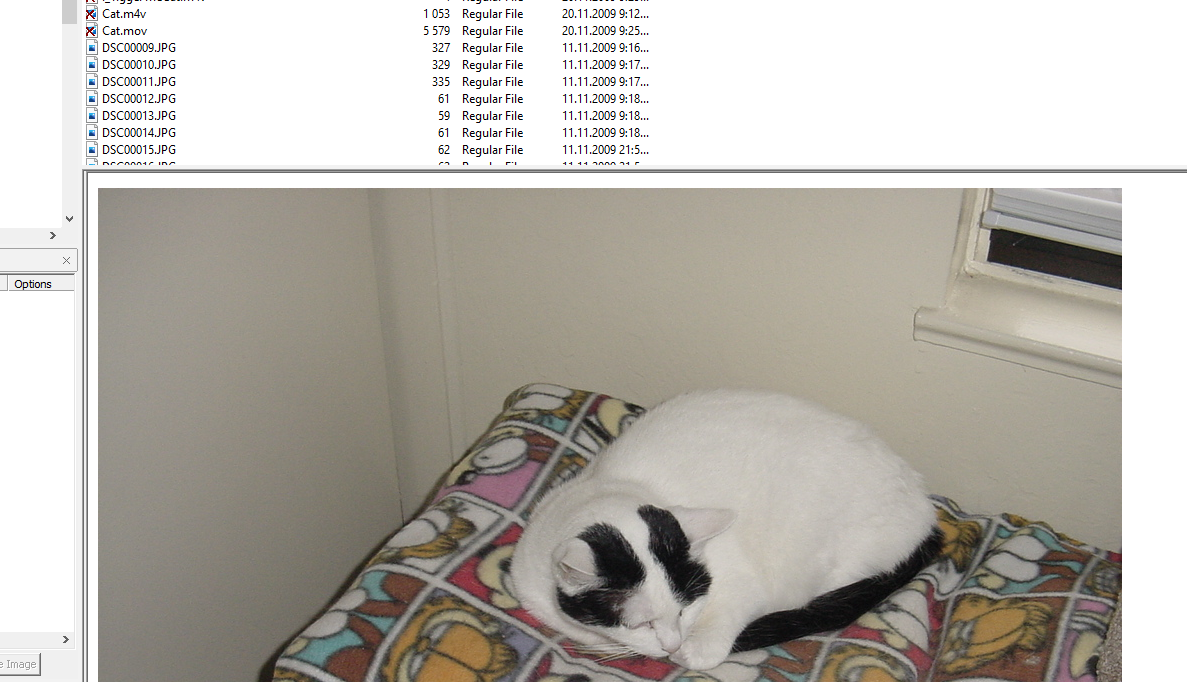
Санкт-Петербург

2020г.

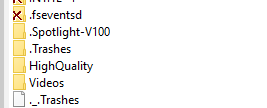
Задача

поиск доказательств, что Jo причастен к корпоративному шпионажу и продаже фото.

Ход выполнения

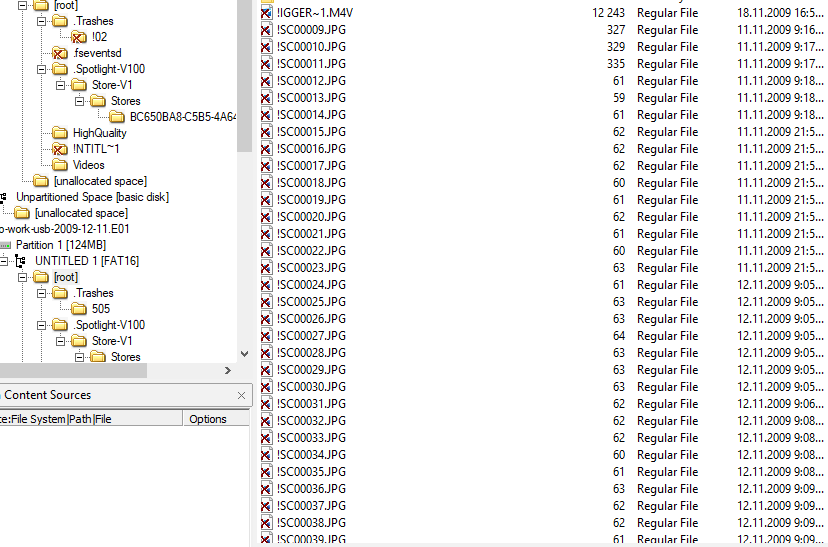
На jo-favorites-usb-2009-12-11.E01 в корневом каталоге обнаружено множество фотографий 

Помимо фотографий найдено несколько каталогов так же содержавший разыскиваемый материал



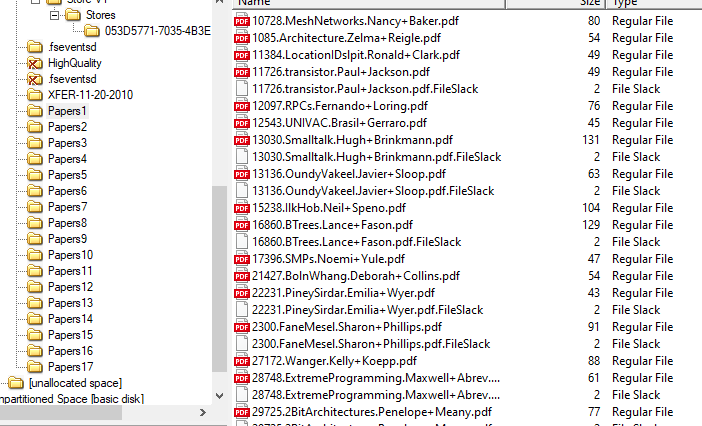
HighQuality содержит фотографии в более высоком разрешении

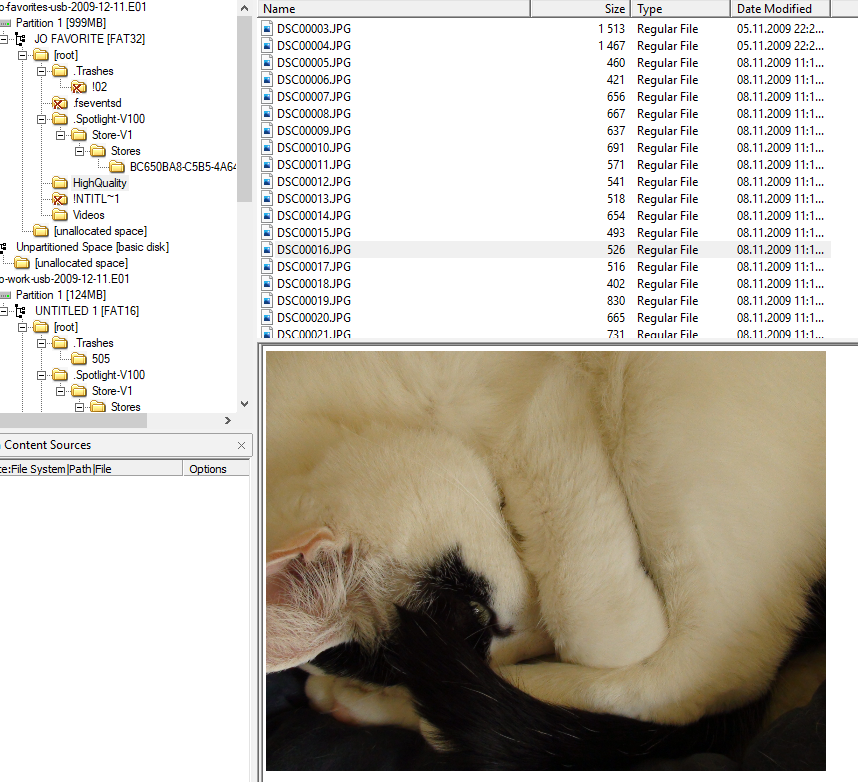
На jo-work-usb-2009-12-11.E01 в корневом каталоге обнаружено множество удаленных файлов



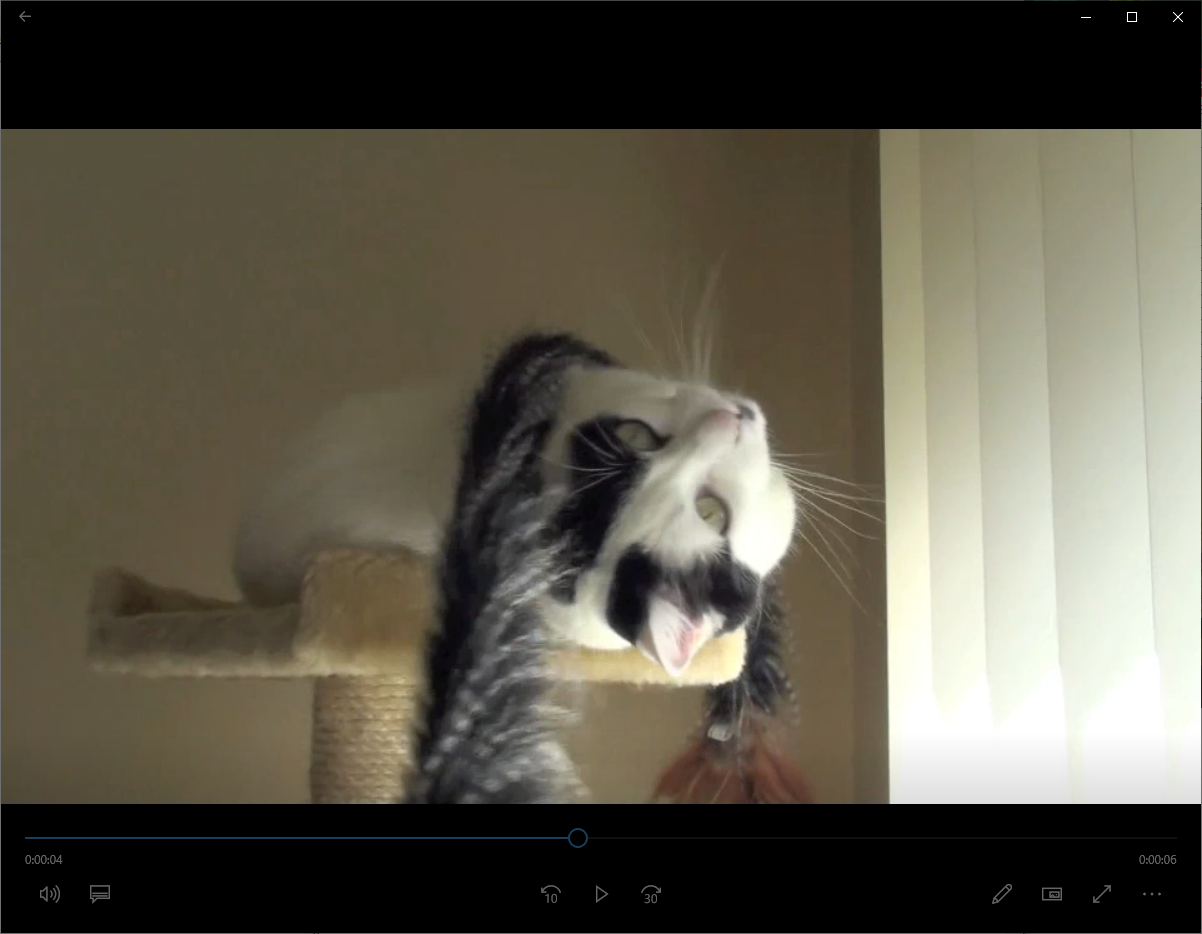
Если использовать специальные инструменты можно восстановить, например на linux можно попробовать dd.

Также материалы, относящиеся к работе.

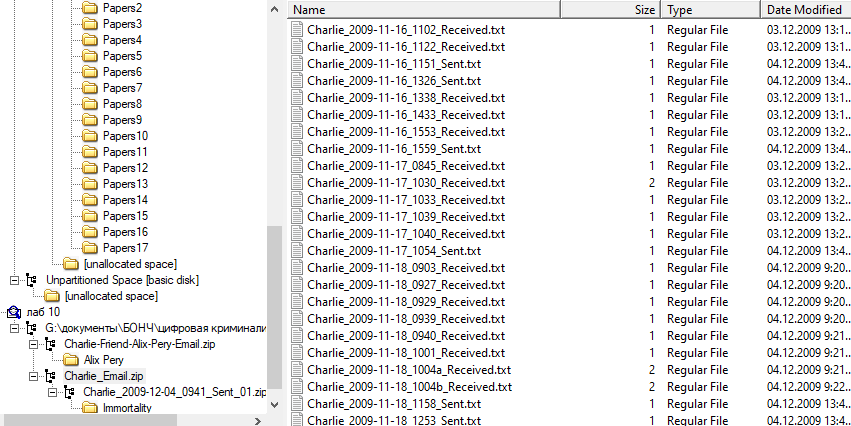




Videos видеоматериалы с кошками



Проверим архив почты, добавим путь к почте



В данных письмах видим, что в первые дни:

* Приветствие
* Новый проект
* Обмен впечатлениями

В письме 11-17-1030 упоминаются конкуренты

«We wouldn't want project2400 to know about our research interests.»

Дальше идет рутинные сообщение и обсуждение кофе

В письме 12-01 1302 следущее сообщение.

Alix,

Pretty soon I'm going to be able to afford to take you on a nice vacation. Where would you want to go if you could name your destination? I'm getting a hot car too.

Charlie

Аликс,

Очень скоро я смогу позволить себе взять тебя в хороший отпуск. Куда бы вы хотели отправиться, если бы могли назвать пункт назначения? Я тоже куплю горячую машину.

Чарли

Он только не давно появился в компании, у него не может быть средств на машину и отпуск.

Далее он получил ответ, согласие.

Alix

Ooh! When will this happen?! I've always wanted to go on a Mediterranean cruise. Should I put a date on my calendar?

Далее он пишет [jaime@project2400.com](mailto:jaime@project2400.com) в письме 12-02 1304

J,

I have something that you'll definitely be interested in. It concerns your competitor. I'm doing a prior art search for them. Want to know what I've found? You know my price. I'll send you the goods after I see half in my account. Make sure you delete this email.

C

У меня есть кое-что, что вас определенно заинтересует. Это касается вашего конкурента. Я провожу для них предварительный поиск. Хотите знать, что я нашел? Ты знаешь мою цену. Я пришлю Вам товар после того, как увижу половину на своем счете. Убедитесь, что вы удалили это письмо.

В сообщении видим, что они давно знакомы и напоминает о своей цене

Далее получает сообщение

This is the Spam & Virus Firewall at mustang.nps.edu.

I'm sorry to inform you that the message below could not be delivered.

When delivery was attempted, the following error was returned.

<jaime@project2400.com>: host mx2.sub3.homie.mail.dreamhost.com[208.97.132.222]

said: 550 5.1.1 <jaime@project2400.com>: Recipient address rejected: User

unknown in virtual alias table (in reply to RCPT TO command)

Reporting-MTA: dns; mustang.nps.edu

Arrival-Date: Wed, 2 Dec 2009 13:05:05 -0800 (PST)

Final-Recipient: rfc822; jaime@project2400.com

Action: failed

Status: 5.0.0

Diagnostic-Code: X-Spam-&-Virus-Firewall; host

mx2.sub3.homie.mail.dreamhost.com[208.97.132.222] said: 550 5.1.1

<jaime@project2400.com>: Recipient address rejected: User unknown in

virtual alias table (in reply to RCPT TO command)

корпоративный фаервол, это позволит извлечь сообщение

далее снова шлет в письме 1325 и получает ответ в письме 0951

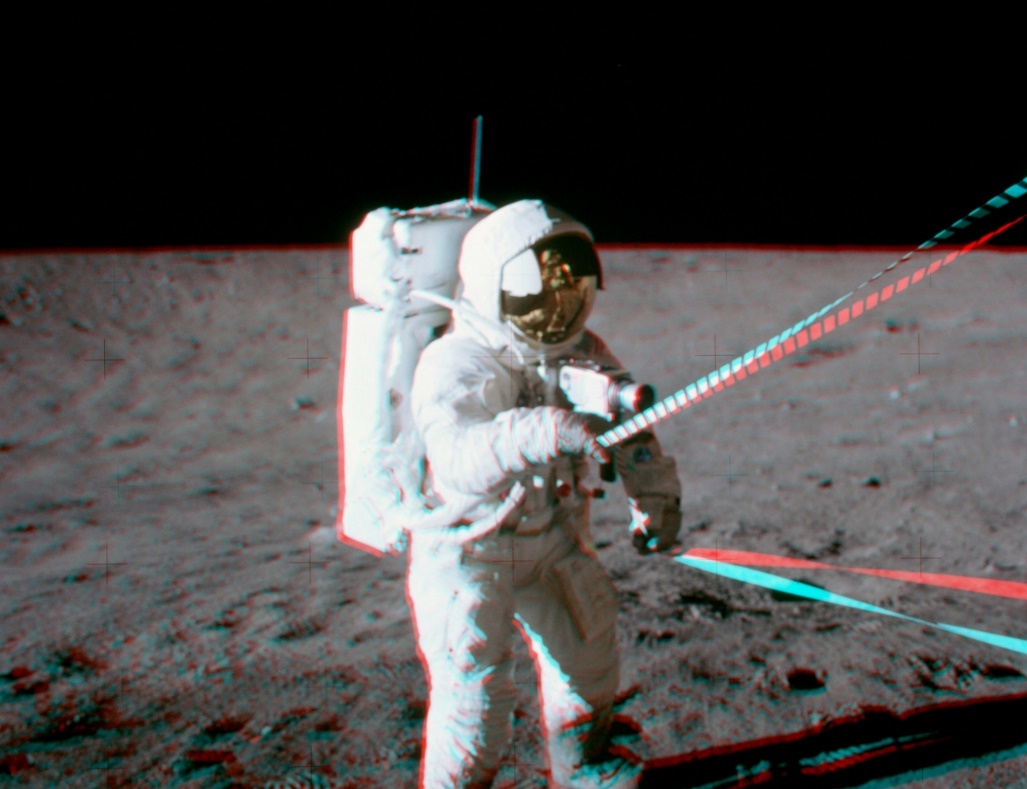
C,

We'll give you 50 large if it's good. I'll put in 10 up front, you'll get

the rest when we see the goods.

J

Далее C отправил письмо 1216\_Sent с фотографией. Однако пришлет инструкции по извлечению, после получения денег



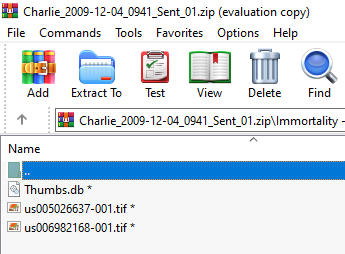
Данные письма уже доказывают что он занимается продажей информации.

В письме 0941

Энди,

К счастью для меня, я просто случайно наткнулся на это. Я нашел предыдущий патент, который определенно аннулирует ваш нынешний патент на бессмертие. Вам следовало бы воспользоваться услугами моего босса, но я просто использую вашу небрежность в своих интересах. Я хочу 100 тысяч, или я обнародую это публично. Мне не нужно говорить вам, как сильно это повредит вашему бизнесу, если я предам это огласке. Не привлекайте полицию, иначе эта информация станет достоянием общественности. Подробнее о том, что я нашел, смотрите во вложении. Я свяжусь со своим банковским номером. Пароль для zip-файла будет скрыт в следующей картинке, которую я вам пришлю.

С





Теперь мы видим шантаж. Нескольких письмах идет подтверждение о отпуске, машине. Все данные письма потверждают кражу и шантаж. Если бы он не использовал корпоративную почту, то шанс на наказание снизилось бы.