

ИНФОРМАТИК **А**

4

Ю.А. Первин

Задумавшись над очередной загогулиной блок-схемы, поднимаю глаза, и взор упирается в сидящую напротив симпатичную девушку. Мысли, конечно, не о ней, а о новом повороте блок-схемы.

15

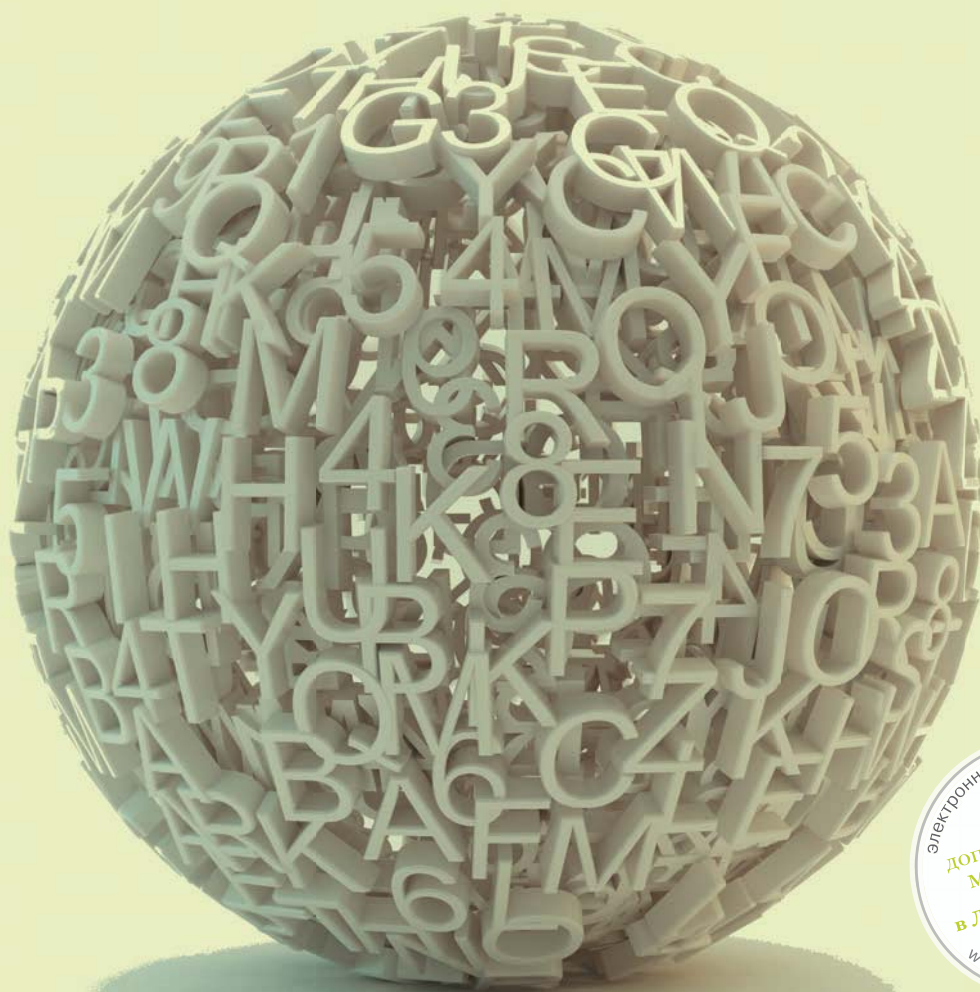
А.А. Дуванов

Какой же была моя радость пополам с удивлением, когда деревяшка заговорила человеческим голосом! Своими руками я сотворил Буратино! Стало понятно, что я волшебник.

38

Д.Ю. Усенков

Словами Огюста Родена... "Нужно взять глыбу мрамора и отсечь от нее все лишнее"





НА ОБЛОЖКЕ

► 3D-принтеры перестали быть экзотикой, увлечением для избранных. Сегодня это вполне промышленный инструмент, используемый в различных областях деятельности. Кстати, среди 3D-принтеров уже имеются и лазерные, и струйные, и даже матричные модели. И стоимость устройств существенно снижается (не резко, но ряд 3D-принтеров уже становится доступен и для домашнего использования). В этом номере мы публикуем подробную статью о текущем состоянии технологий 3D-печати. Может быть, дождемся мы и появления “Информатики” в 3D-версии ©.

В НОМЕРЕ

- 3** ПАРА СЛОВ
 - Не знаю!
- 4** ИНФОРМАТИКА В ЛИЦАХ
 - Ю.А. Первин
 - А.А. Дуванов
- 26** ЕГЭ
 - Люблю ЕГЭ за В15, или Еще раз про метод отображения
- 33** ОЛИМПИАДЫ
 - Школьники играют в СТГ
- 38** ТЕХНОЛОГИИ
 - Что такое 3D-принтер и как он работает
- 48** ЗАНИМАТЕЛЬНЫЕ МАТЕРИАЛЫ ДЛЯ ПЫТЛИВЫХ УЧЕНИКОВ И ИХ ТАЛАНТЛИВЫХ УЧИТЕЛЕЙ
 - “В мир информатики” № 199

В ЛИЧНОМ КАБИНЕТЕ

Облачные технологии от Издательского дома “Первое сентября”

Уважаемые подписчики бумажной версии журнала!

Дополнительные материалы к номеру и электронная версия журнала находятся в вашем Личном кабинете на сайте www.1september.ru.

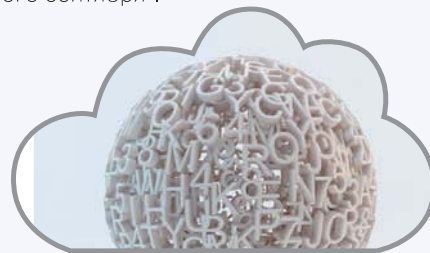
Для доступа к материалам воспользуйтесь, пожалуйста, кодом доступа, вложенным в этот номер (№7–8/2014).

Срок действия кода: с 1 июля по 31 декабря 2014 года.

Для активации кода:

- зайдите на сайт www.1september.ru;
- откройте Личный кабинет (создайте, если у вас его еще нет);
- введите код доступа и выберите свое издание.

Справки: podpiska@1september.ru или через службу поддержки на портале “Первое сентября”.



ЭЛЕКТРОННЫЕ МАТЕРИАЛЫ
Презентации к статьям номера

ИНФОРМАТИКА

ПОДПИСНЫЕ ИНДЕКСЫ
по каталогу “Почта России”: 79066 — бумажная версия, 12684 — электронная версия

<http://inf.1september.ru>

Учебно-методический журнал для учителей информатики
Основан в 1995 г.
Выходит один раз в месяц

РЕДАКЦИЯ:
гл. редактор С.Л. Островский
редакторы

Е.В. Андреева,
Д.М. Златопольский
(редактор вкладки
“В мир информатики”)

Дизайн макета И.Е. Лукьянов
верстка Н.И. Пронская
корректор Е.Л. Володина
секретарь Н.П. Медведева
Фото: фотобанк Shutterstock
Журнал распространяется по подписке
Цена свободная
Тираж 27 622 экз.
Тел. редакции: (499) 249-48-96
E-mail: inf@1september.ru
<http://inf.1september.ru>

ИЗДАТЕЛЬСКИЙ ДОМ
“ПЕРВОЕ СЕНТЯБРЯ”

Главный редактор:
Артем Соловейчик
(генеральный директор)

Коммерческая деятельность:
Константин Шмарковский
(финансовый директор)

Развитие, IT
и координация проектов:
Сергей Островский
(исполнительный директор)

Реклама, конференции
и техническое обеспечение
Издательского дома:

Павел Кузнецов

Производство:
Станислав Савельев

Административно-
хозяйственное обеспечение:
Андрей Ушков

Педагогический университет:
Валерия Арсланян (ректор)

ЖУРНАЛЫ ИЗДАТЕЛЬСКОГО ДОМА
“ПЕРВОЕ СЕНТЯБРЯ”

Английский язык – А.Громушкина
Библиотека в школе – О.Громова
Биология – Н.Иванова
География – О.Коротова
Дошкольное образование – Д.Тюттерин
Здоровье детей – Н.Сёмина
Информатика – С.Островский
Искусство – О.Волкова
История – А.Савельев
Классное руководство
и воспитание школьников –
М.Битянова

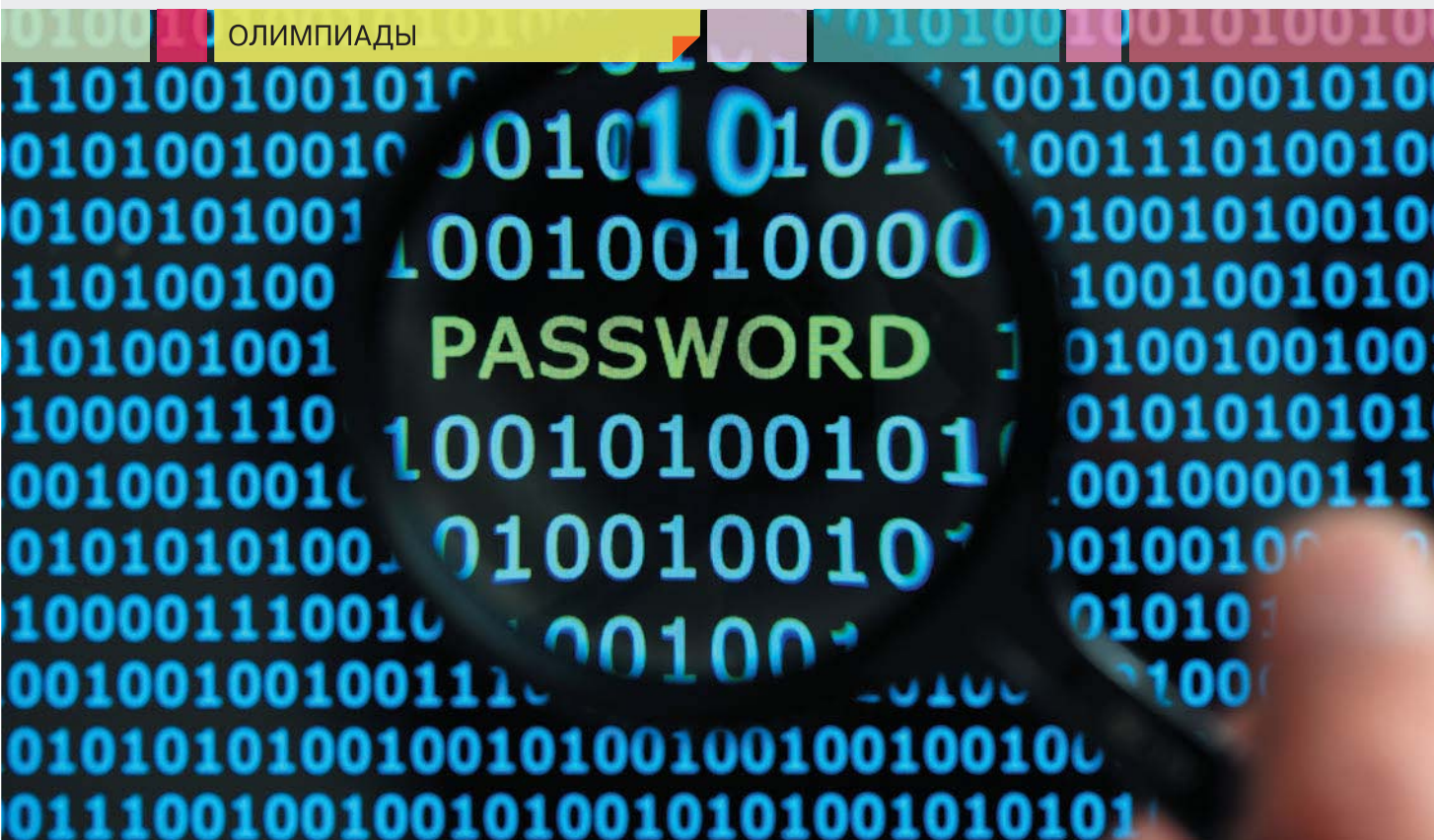
Литература – С.Волков
Математика – Л.Рослова
Начальная школа – М.Соловейчик
Немецкий язык – М.Бузоева
ОБЖ – А.Митрофанов
Русский язык – Л.Гончар
Спорт в школе – О.Леонтьева
Технология – А.Митрофанов
Управление школой – Е.Рачевский
Физика – Н.Козлова
Французский язык – Г.Чесновицкая
Химия – О.Блохина
Школа для родителей –
Л.Печатникова
Школьный психолог – М.Чибисова

УЧРЕДИТЕЛЬ:
ООО “ЧИСТЫЕ ПРУДЫ”

Зарегистрировано
ПИ № ФС77-44341
от 22.03.2011
в Министерстве РФ
по делам печати
Подписано в печать:
по графику 20.05.2014,
фактически 20.05.2014
Заказ №

Отпечатано в ОАО “Первая
Образцовая типография”
Филиал “Чеховский Печатный Двор”
ул. Полиграфистов, д. 1,
Московская область,
г. Чехов, 142300
Сайт: www.chpd.ru
E-mail: sales@chpk.ru
Факс: 8 (495) 988-63-76
АДРЕС ИЗДАТЕЛЯ:
ул. Киевская, д. 24,
Москва, 121165
Тел./факс: (499) 249-31-38

Отдел рекламы:
(499) 249-98-70
<http://1september.ru>
ИЗДАТЕЛЬСКАЯ ПОДПИСКА:
Телефон: (499) 249-47-58
E-mail: podpiska@1september.ru



Школьники играют в CTF

В.В. Ильин, лицей
“Вторая школа”,
В.А. Павленко,
ГБОУ Школа-интернат
“Интеллектуал”

Хотите простую задачу?
МОЕ условие: Ежей 9, а ушей?..

ОТВЕТ:

Восемнадцать? И при чем здесь ежи?

Нет. Задача простая, но не совсем.
Решение — в статье.

На старт!

Известно много задач по алгоритмам и программированию, по этим задачам проводятся олимпиады. А вот задачи и конкурсы по компьютерным технологиям встречаются редко. На самом деле надо лишь знать, где их искать.

CTF (*Capture The Flag*) — это командные соревнования по компьютерной безопасности. Появились они в США уже давно (более 20 лет назад), а в России впервые были проведены на Урале в 2006 году. CTF существует в двух основных вариантах: классический CTF (атака-

защита сервера) и тасковый (task-based) CTF. Второй вариант более доступен школьникам, о нем мы и расскажем.

В тасковом CTF командам дается набор заданий (тасков) из разных категорий и областей знаний. Например, это могут быть задания на криптографию, стеганографию, веб-технологии. Команда пытается решить их любым доступным образом, применяя свои навыки работы с компьютерами или приобретая их по ходу соревнования. Результатом решения является некий ключ (он называется флаг), который и необходимо отправить на проверку.

Для школьников, во всяком случае в России, эти соревнования начали проводиться лишь пару лет назад. А ведь компьютерно-детективные загадки — это очень здорово.

Конечно, немногие школьники хорошо разбираются в современных алгоритмах шифрования, владеют различными способами работы с изображениями или аудиофайлами и знают подробности функционирования Интернета. От участников

требуется не столько владеть знаниями, сколько уметь быстро их получать из Интернета: из статей, документации, литературы. Знания приходится тут же применять на практике.

С начала и до конца марта этого года в Интернете проводилась UFO CTF School — открытая олимпиада Южного федерального университета по информационной безопасности среди школьников. В первых трех частях нашей статьи мы расскажем о некоторых задачах этого конкурса.

На момент написания статьи задачи олимпиады доступны по адресу: <http://ufologists.ictis.sfedu.ru/game>, — но отправлять флаги в проверяющую систему уже нельзя. Обычно CTF-площадки закрываются через некоторое время после проведения соревнования, потому что их поддержание в рабочем состоянии требует сил. Для проведения CTF нужно не только опубликовать условия задач. Некоторые задачи заключаются в анализе сетевых сервисов: сайтов, удаленных компьютеров, и от организаторов конкурса требуется поддерживать их работоспособность.

Некоторые задачи доступны постоянно, например, на сайтах:

<http://5kr.mosuzedu.ru/CTFtasks>

<https://picocft.com/>

<https://ctf.fluxfingers.net/2013/challenges>

Разгон!

Base64

Декодируй это: “ZmxhZ3s2Y2FiOGNlMjRkNTNkYzQ1MGFiNTU0MDliZWZWM2ZTQ1Mn0”.

Что такое Base64? Идем в Википедию. “Эта система широко используется в электронной почте для представления бинарных файлов в тексте письма (транспортное кодирование). Все широко известные варианты, известные под названием “Base64”, используют символы A–Z, a–z и 0–9, что составляет 62 знака, для недостающих двух знаков в разных системах используются различные символы”.

Первой ссылкой в поисковиках по запросу “Base64” видим “Online Base64 декодер”. Технически задача оказывается очень простой — скопируем текст в окошко декодера и получим флаг.

Что же, задачи CTF такие простые, и надо лишь искать перекодировщики между разными форматами? Конечно, нет. Но даже такая простая задача могла быть сложнее. Например, названия кодировки могло не быть в условии, и тогда нужно было бы выяснять, какая именно кодировка используется.

Главное, что в процессе решения у неопытного школьника произойдет знакомство с новой технологией из компьютерного мира. А дальше когда-нибудь он может встретить Base64 как одну из технологий в реальном большом проекте. Например, при передаче данных по сети. И тогда уже школьник сможет спра-

виться с более сложной задачей: например, получить доступ к плохо защищенному веб-сервису.

Veni vidi vici

Что же это: “Wkh Txlfn Eurzq Ira Mxpsv Ryhu Wkh Odcb Grj”?

Это уже не просто кодирование, а шифрование. Нужно догадаться, что это за шифр, и расшифровать сообщение. “Пришел, увидел, победил” — фраза Юлия Цезаря. А перед нами шифр Цезаря: алфавит записывается по кругу, и каждая буква меняется на своего соседа справа на расстоянии k букв. Как узнать, чему равно k в нашем случае? Это можно решить подбором (в худшем случае мы попробуем 25 вариантов). Поскольку шифр Цезаря очень известен, то в Интернете есть его дешифровщики: например, <http://online-calculators.appspot.com/caesar/>.

Можно написать и свой дешифровщик на Питоне.

```
text = list(input('Enter message: '))
lowercase = list('abcdefghijklmnopqrstuvwxyz')
uppercase = list('ABCDEFGHIJKLMNOPQRSTUVWXYZ')
key = int(input('Enter key: '))
cipher = []
for c in text:
    if c in lowercase:
        cipher.append(lowercase[(lowercase.
index(c) - key) % (len(lowercase))])
    elif c in uppercase:
        cipher.append(uppercase[(uppercase.
index(c) - key) % (len(uppercase))])
    else:
        cipher.append(c)
print('Your decrypted message is:',
''.join(cipher))
```

А вот простая задача по другой теме.

CookieMonster

КукиМонстру нужны печенки!

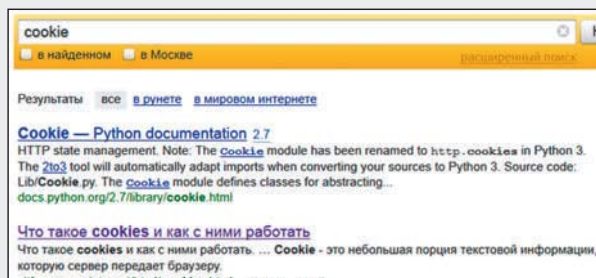
<http://188.226.160.200:802/>

По ссылке открывалась картинка

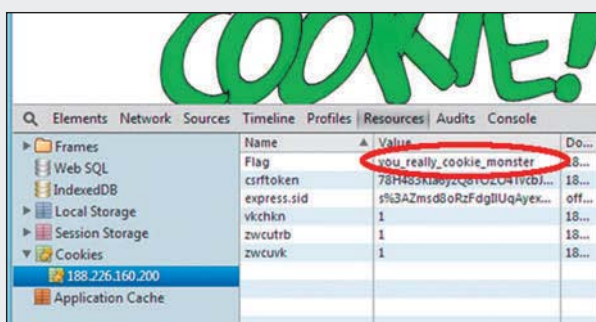


Пытаемся искать скрытый текст на картинке, анализируем количество дырочек в печенье, гуглим имя персонажа из мультфильма — ничего интересного. Как же накормить это забавное существо?

Cookie...



Ага! Может быть, имеются в виду веб-куки? Читаем статью и смотрим куки на страничке с картинкой — это можно сделать стандартными средствами любого браузера. Гуглим так: “как посмотреть cookie chrome”.



AdminPanel

Попробуй зайти в админку и получи флаг!
<http://188.226.160.200:801/>

На сайте по ссылке есть единственная картинка-ссылка, при переходе по которой мы попадаем на страничку с текстом “go away, stranger!”.

Опять просматриваем куки. Оказывается, страница устанавливает куки с ключом admin и значением false. Учимся подменять куки при запросах к сайтам. Это можно сделать из JavaScript-консоли разработчика в браузере одной командой:

```
document.cookie = 'admin=true'
```

Перезагружаем страничку — и флаг наш. Разумеется, куки запросов можно подменять многими другими способами, о которых в Интернете написано немало.

Украденный телефон

Еще в одной задаче дана фотография вместе с таким текстом:

“В Москве у меня украли телефон ☹. Хорошо, что все новые фотографии синхронизируются с моим dropbox. Эта фотография сделана совсем недавно — помоги мне узнать, в каком городе сейчас вор?”

На фотографии русско-английский разговорник. Чем это может помочь?

Оказывается, что разговорник тут ни при чем. Для решения задачи нужно достать из фотографии так называемую “EXIF-информацию”, а вернее, геоданные из нее. Фотокамеры записывают в геоданных внутри файла с картинкой координаты места, в котором был сделан снимок. Посмотреть EXIF можно стандартными средствами Windows (выбираем в Проводнике в контекстном меню пункт Свойства файла). Потом можно вбить полученные

данные широты и долготы в Гугл-карты и попасть в загаданный город.

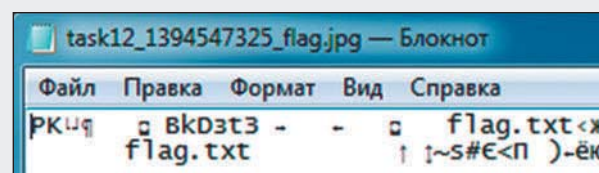
Очень удобен для решения этой задачи онлайн-сервис <http://regex.info/exif.cgi>, он позволяет загрузить картинку и сразу показывает нужный участок географической карты.

Что не так с моей картинкой?

Дана ссылка на картинку, но при переходе по ссылке картинка не открывается, а браузер пишет об ошибке.

Попробуем открыть картинку нестандартными средствами. Лучше всего подходят для исследования внутренней структуры файлов специальные hex-редакторы, например, 010 Editor (<http://www.sweetscape.com/010editor/>). Такие редакторы позволяют анализировать каждый бит содержимого файла.

Для исследования этой задачи подойдет даже обычный Блокнот. Скачиваем файл правой кнопкой мыши (Сохранить объект как) и открываем в Блокноте.



Видим начальные символы PK и строку flag.txt.

По запросу “pk file” Гугл подсказывает, что PK — это сигнатура zip-архивов. Первые два байта в каждом zip-архиве — это символы “PK”. Похоже, нам дали архив под видом картинки: случай, когда “обложка” не соответствует содержимому.

Меняем расширение файла на zip и стандартно открываем. В архиве обнаруживаем файл *flag.txt*. Если у вас Windows и в Свойствах папки стоит галочка “Скрывать расширение у зарегистрированных типов файлов”, то сначала вам нужно будет снять эту галочку. Только после этого вы сможете изменить расширение имени файла из Проводника.

Быстрее!

Не все задачи решаются просто.
Например,

Anonymous

Дается изображение — файл JPEG.

Замечаем, что изображение подозрительно долго грузится. Действительно, файл занимает на диске 7 мегабайт, хотя обычно картинки такого же размера по ширине и высоте занимают сотню килобайт.

Смотрим в hex-редакторе содержимое файла. В конце файла видим что-то странное и непохожее на “хаотичное” содержание jpg:

```
/9j/4AAQSkZJRgABAQEAYABgAAD/  
4RvvRXhpZgAASUkqAAgAAAAMAA4BAG...
```

Это Base64? Тогда декодируем его и посмотрим на результат.

В начале декодированных данных видим “JFIF” — сигнатуру формата JPEG. Стало быть, в одной картинке была сокрыта другая.

Формат JPEG — вообще идеальное место для хранения тайной информации от неискушенных пользователей (искусшенные сразу откроют картинку в hex-редакторе, и секрет раскроется). Дело в том, что в файле этого формата есть маркер конца изображения, и просмотрщики обычно игнорируют все, что следует после него. Если мы хотим послать скрытые данные внутри картинка, то просто приписываем в конец файла любые символы.

Вернемся к заданию. На второй картинке флага нет. Зато в hex-редакторе снова видим Base64 в конце файла. Снова выцепляем и декодируем, и снова картинка, и снова Base64 в конце файла. 7 мегабайт оказываются спрятанными друг в друга семью картинками. Матрешка! На самой внутренней картинке — флаг.

Для автоматизации процесса можно написать скрипт, хотя и без него задача решается.

Вот shell-скрипт:

```
for i in `seq -w 1 6` ; do
    strings -n 1000 file$i.bin |
    base64 -D > file$((i + 1)).bin
done
```

Кстати, ответ на задачу в начале статьи: AAF.

Сообщение набрано русскими и латинскими буквами. Это можно увидеть по небольшой разнице в изображении символов, а на мысль о необычном наборе наводит слово “MOE”, набранное прописными и с нулем вместо “O”. Для того чтобы ее смогли решить и читатели печатной версии, мы набрали текст разными шрифтами. От этого задача стала проще, но неаккуратнее. Обычно подобные задачи оформляют так, что на первый взгляд разница незаметна.

MOE условие: Ежей 9, а ушей?.. **ОТВЕТ:**

Если оставить только латинские буквы и цифры, получится строка MOEueE9yOTBE, и если ее декодировать как Base64, получится 3A2x0r90D, то есть $3A2_{16} \oplus 90D_{16}$, а это AAF₁₆.

Call me

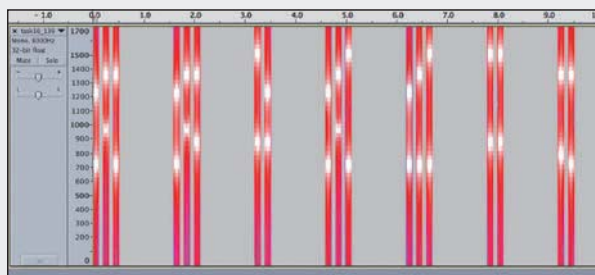
Нам поступил странный звонок. Можешь разобраться, в чем дело?

К заданию приложен wav-файл.

На записи слышен характерный звук набираемых на телефоне клавиш. По запросу “телефон тональный режим код” легко узнать, что при кодировании в тональном режиме используется Dual-Tone Multi-Frequency: система, при которой каждый сигнал передается как сумма двух частот из фиксированного набора:

1	2	3	A	697 Гц
4	5	6	B	770 Гц
7	8	9	C	852 Гц
*	0	#	D	941 Гц
1209 Гц	1336 Гц	1477 Гц	1633 Гц	

Откроем наш аудиофайл в Audacity и выберем для дорожки режим показа Spectrogram:



По оси ординат — частота в герцах. Одна вертикальная полоска на спектрограмме — одно нажатие клавиши. Каждая вертикальная полоска имеет два засвета: нижний задает строку в кодовой таблице, верхний — столбец. Считав коды по засветам, получаем

102-108-97-103-123-99-42-108-108-95-109-51-95-100-107-100-51-125

Переводим эти номера в символы по таблице ASCII и получаем флаг.

Совсем быстро!

Решение некоторых задач требует серьезной подготовки от участников.

Was ist das?

Дана фотография мельницы с огромной надписью “Was ist das?”.

Опыт подсказывает: мельница тут ни при чем. А в правом нижнем углу видна подсказка.



Перед нами изображение формата bmp без сжатия. Красный, зеленый, синий в подсказке — информация спрятана в битах.

Обычно для сокрытия информации в изображении используют младшие биты цветовых каналов. Изменение значения цветового канала на единичку незначительно, поскольку неразличимо для глаза. В этой задаче информация скрывается в разных битах, поэтому видны искажения. Если приглядеться, в самой верхней строке видны “артефакты” — цветные точки, выбивающиеся из фона картинка.

Извлечь флаг технически сложно. Тут уже без серьезных навыков программирования не обойтись. Из

красного канала нужно взять младший бит, из зеленого — второй и так собрать текст флага. Решающему эту задачу придется найти какую-нибудь библиотеку, которая достает данные из картинок, и написать с ее помощью программу, собирающую решение задачи.

Блокнотик

Самый надежный шифр — это одноразовый блокнот, но мне лень придумывать много...

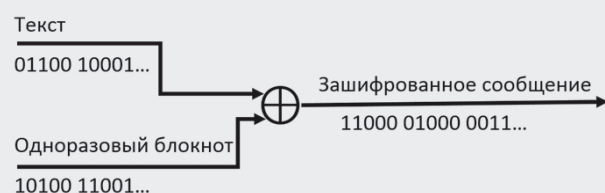
```
2426d6c3ef1a29652be80311a82c031d3ba564992
d2fbf1d3bb3bee6cb523187e64ecb1af636b0a492571
de1ac693ca1048373bee37912ccf544233c5507f14a14
a8da2877a2b0d16a8cb90ce91bc0192fe733b4b254e8
34b943bf41278cf922314c9f8433
```

```
242193b0cf1d236520ff145ce339140b69ec65dc2c
2fbe0f77abf0f08e502885e759db1af62bf1bc834154f0
e97b3ae445897d71f965128df456232e5210f15615be
8e3460b8e5cc65d8a35eff0d94153aec22b0b54aba20
b90ba24d2796f4226559879571
```

... (в задании приводится еще пять строк такого же вида).

Одноразовый блокнот — это шифр, при котором текст зашифровывается и расшифровывается одним и тем же ключом. Исходный текст для шифрования представляется как набор битов. Затем берется ключ — двоичная строка длиной с текст — и побитово ксорится (операция “исключающее или”) с текстом:

$$\text{cipher} = \text{text} \oplus \text{key}$$



Расшифровка проста: ксорим зашифрованный текст с ключом. Поскольку для каждого бита выполняется $\text{key} \oplus \text{key} = 0$ (это свойство операции “исключающее или”), то $\text{cipher} \oplus \text{key} = \text{text} \oplus \text{key} \oplus \text{key} = \text{text}$.

Одноразовый блокнот — идеальный шифр, т.е. его в принципе нельзя взломать. Если, конечно, использовать ключ только один раз в жизни. В нашем же случае на одном ключе зашифровано семь разных текстов. Поэтому можно применить частотный анализ и постепенно расшифровать все сообщения.

Естественно, и при решении этой задачи без программирования не обойтись.

Полностью решение этой задачи можно почитать на странице <http://lights-out-ctf.ghost.io/ufo-ctf-school-2014-quals-bloknotik/>.

Выход в третье измерение

В этом году мы в Москве проводили очный CTF для школьников, который организовала известная уральская CTF-команда Хакердом. Задачи были сложнее, чем “уфошные”, соревнование длилось весь день (восемь часов с перерывом на обед). Мы в Москве решили для желающих устроить допол-

нительные конкурсы на задачах с материальными объектами, чтобы уставшие участники могли хотя бы на время вырваться в реальный мир из двумерности монитора.

Наибольшим успехом, пожалуй, пользовались задачи на станции RealAdmin Corner (админский уголок).

Например, таск **How Long**.

Участникам давался большой моток витой пары и десятисантиметровая линейка. Требовалось измерить длину мотка.

Тем, кто начинал с энтузиазмом наматывать витую пару на локоть, мы замечали, что погрешность измерений должна составить не более двух сантиметров.

Решение: Достаточно было заметить на проводе заводские надписи-маркеры с отсчетами длины: “0002FT”, “0004FT”, “0006FT” и т.д. (это отсчеты в футах). Затем нужно было узнать длину фута, а также померить расстояния от концов провода до ближайших к ним маркеров.

Или таск посложнее:

Your IP

Дается ноутбук и роутер. На роутере отключен WiFi, но есть витая пара, концы и обжиматель сетевого кабеля.

Решение: правильно обжимаем провод с двух сторон, коннектимся к роутеру по полученному кабелю и получаем IP по DHCP.

Естественно, как и при решении задач основного соревнования, участникам разрешалось пользоваться интернет-поисковиками.

Продолжаем движение!

Конечно, CTF-соревнование — лишь “затравка”, после которой школьникам следует более глубоко изучить различные прикладные разделы информатики. Но интерес — это очень важный стимул к обучению.

Мы уверены, что даже после простого чтения нашей статьи уровень компьютерной грамотности каждого читателя в чем-то вырос. А уж тем более он сильно вырастает у школьников, которые не читают решения, а пытаются сами “штурмовать” задачи и получают новые знания в процессе. Кстати, от решения задач часто невозможно оторваться, а задачи достаточно сложны, поэтому взрослые таксовые CTF-соревнования обычно проводят длиной в 48 часов.

CTF — это игра и это начало серьезного образования. Далеко не все участники станут специалистами в области компьютерной безопасности, но вкус к более глубокому изучению компьютерных технологий появится у многих.

Вместо заключения еще одна задача!

Бывают и задачи-шутки. Попробуйте решить такую:

Ремингтонист

Оо. Что это? “trdcv utfcvvh iuhbnmk 0okm”

Подсказка. Компьютер сильно помогает решить эту задачу. Особенно выключенный.