Виртуальные следы в криминалистике

Выполнил студент 4 курса
Струнский А.Д.

- **Владимир Алексеевич Мещеряков** (19 июня 1963) — российский криминалист, доктор юридических наук (2001), кандидат технических наук (1992), профессор (2006), член-корреспондент РАЕН (2007),

Виртуальные следы - это

- любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами

Классификации

- **По типу физического носителя:**
- 1) следы на жестком диске (винчестере), магнитной ленте (стримере), оптическом диске (CD, DVD), на дискете (флоппи диске);
  2) следы в оперативных запоминающих устройствах (ОЗУ) ЭВМ;
  3) следы в ОЗУ периферийных устройств (лазерного принтера, например);
  4) следы в ОЗУ компьютерных устройств связи и сетевых устройств;
  5) следы в проводных, радио-оптических и других электромагнитных системах и сетях связи

Классификации

- **По месту их нахождения:**
  1) следы на компьютере преступника;
  2) следы на "компьютере-жертве".
  На "компьютере-жертве" это:
  а) таблица расширения файлов (FAT, NTFS или другая в зависимости от типа используемой операционной системы);
  б) системный реестр операционной системы;
  в) отдельные кластеры магнитного носителя информации (винчестера, дискеты), в которых записываются фрагменты исполняемых файлов (программ) и файлов конфигурации;
  г) файлы и каталоги (папки) хранения входящей электронной почты и прикрепленных исполняемых файлов, конфигурации почтовой программы;
  д) файлы конфигурации программ удаленного соединения компьютера с информационной сетью

Koobface

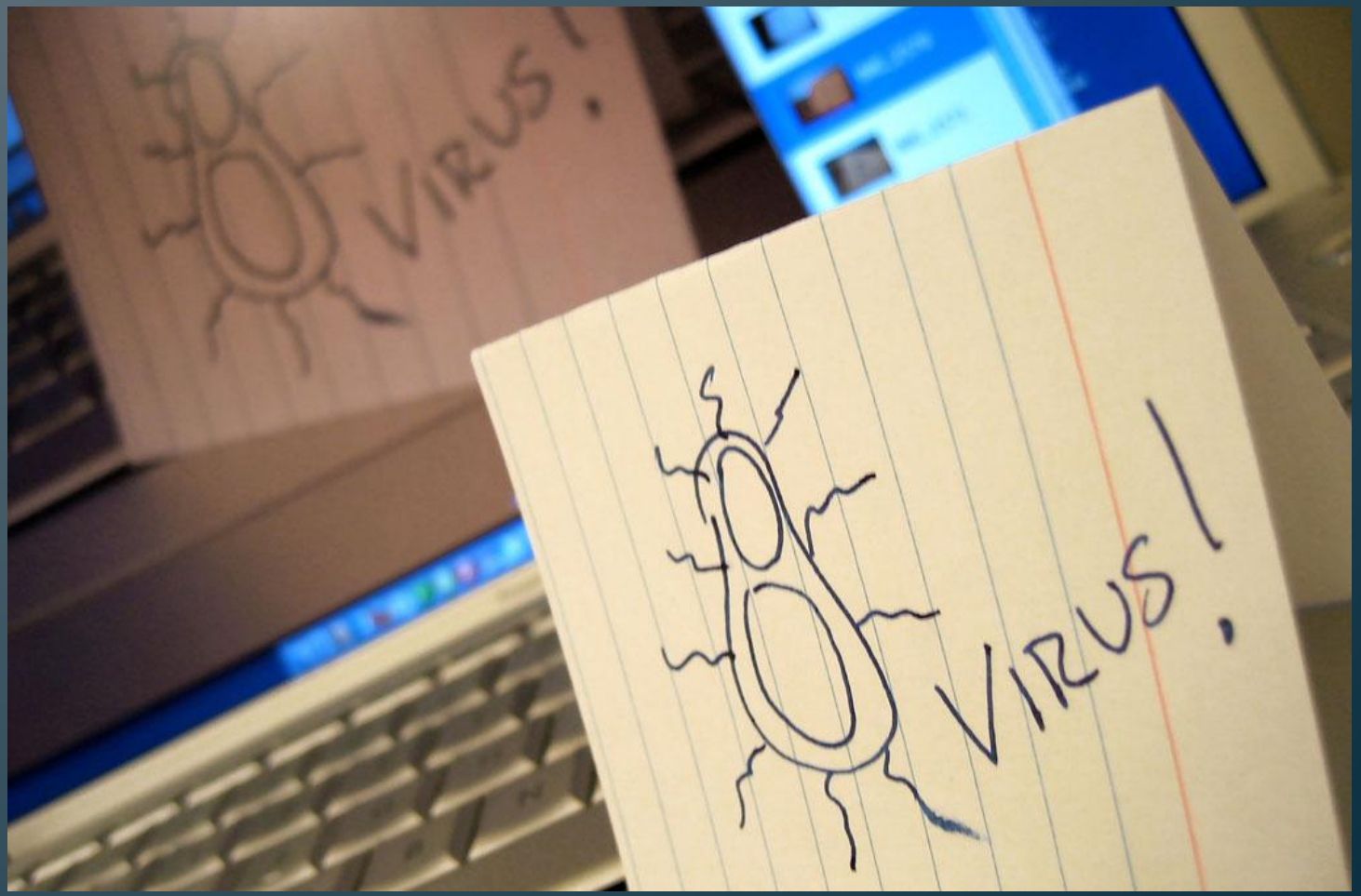
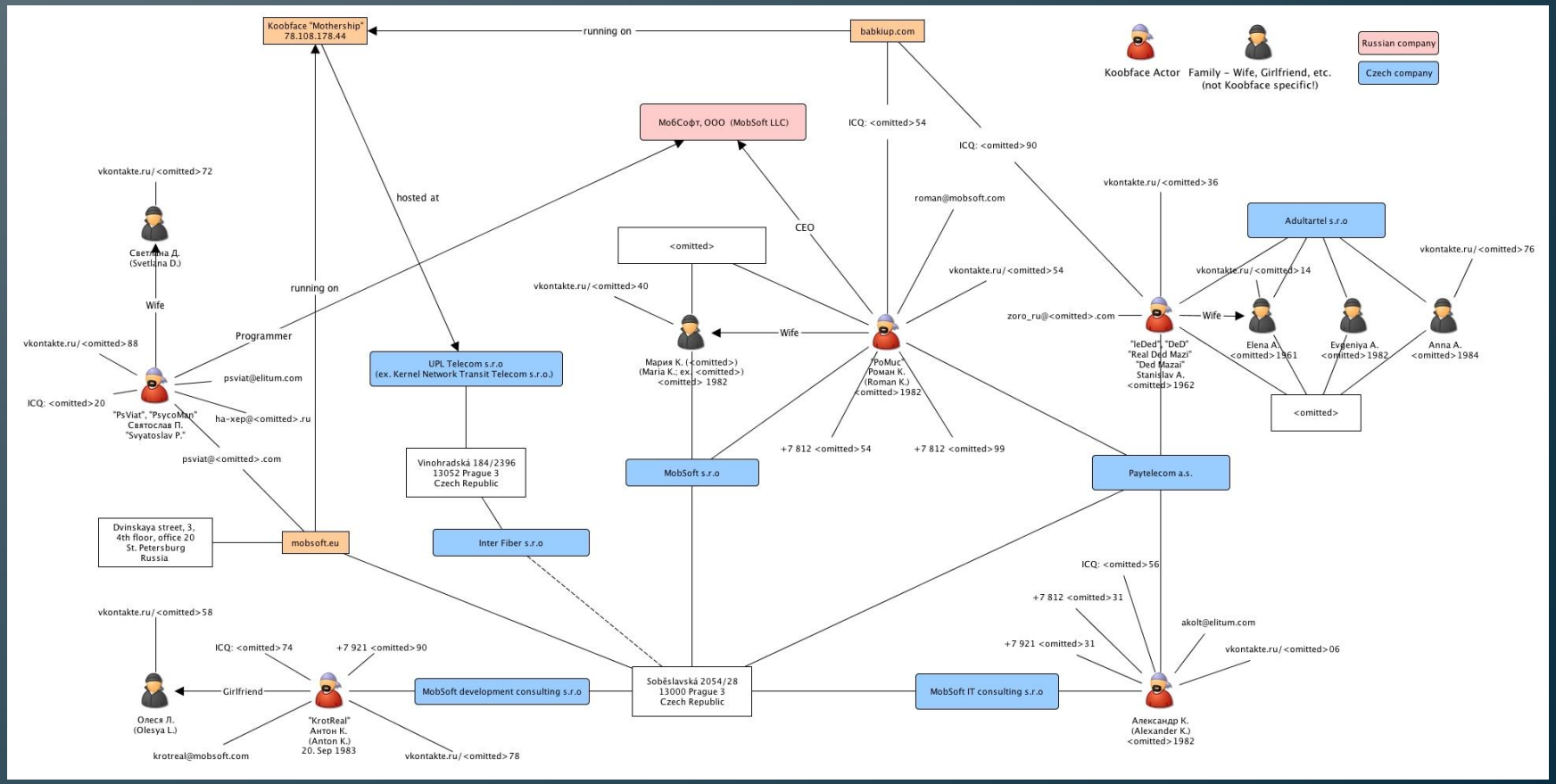


Схема следов



stats_sms.php (no symbol selected)

```php
<?
    $phones = array(
        // phone => array(Sun, Mon, .., Sat)
        '+7911      22' => array('1100', '1000', '1000', '1000',
//      '+7921      31' => array('1200', '1200', '1200', '1200',
        '+7921      99' => array('1000', '0900', '0900', '0900',
        '+7921      90' => array('1300', '0930', '0930', '0930',
        '+7911      68' => array('1100', '1000', '1000', '1000',
    );
```

```php
//########## KrotReal 04-08-2009
function get_blogger_domain () {

    $mysql_link = mysql_connect("localhost", "root", "turbologin
    mysql_select_db("myspace", $mysql_link);

    $sql = "SELECT * FROM blogger WHERE blogname != '' AND count
    $q = mysql_query($sql);
    if (mysql_num_rows($q) <= 0) {
        $sql = "SELECT * FROM blogger WHERE blogname != '' ORDER
        $q = mysql_query($sql);
        while ($arr = mysql_fetch_array($q)) {
```

```
                mv /tmp/restore/${array[1]} ${array[3]}
            fi
        elif [ "${array[0]}" = "l" ]; then
            ln -s ${array[2]} ${array[1]}
        fi
        chown -R leded:leded /work/
done

crontab /tmp/restore/cron/crontab
```


Nevskiy prospekt
Goncharnaya ulitsa
Poltavskaya ulitsa
Poltavskaya ulitsa
Tovarnyy pereulok
Red Club

Спасибо за внимание!

«Анонимности нет, смиритесь» ©