Digital Forensics

or

Your trail is easier to follow than you think

Jim Lyle
NIST
Information Technology Laboratory
Software & Systems Division

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this talk in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

A Tasty Case

- Natasha Romanov (former secret agent) has retired and opened a new Russian Tea Room on Lubyanka Square in Moscow.
- However, her employee Nick Ulyanov has vanished and may have stolen her award winning menu.
- The last he was seen, he was hovering near the computer with a flash drive in his hand.
- Natasha suspects that Nick copied her award winning menu to the flash drive and plans to open his own Tea Room in Saint Petersburg with his own version of Natasha’s award winning menu.

Call The Cops

- Natasha has called her cousins, Andrew & Sasha Demidov, who also happen to be a crack digital forensics team for the Metropolitan Moscow Police.
- They get a warrant & stake out the Train Station and watch the outbound trains.
- The Chief also gives them his wife’s brother’s seventh son, the department intern, Ivan Durok, with the comment “be nice to him, try to teach him the skills, don’t let him contaminate the evidence, no, you can’t shoot him, and I owe you guys one.”
- They catch Nick about to board the express to Saint Petersburg.
- Now what . . .

First Look

- A search of the suspect reveals a flash drive
- Bag & Tag – Start chain of custody to document who has the drive
- Forensic image (or copies made)
- Ivan wants to take a look, Andrew gives one of the copies to Ivan. He inserts it into his laptop and sees just one file. It’s not the missing menu. Ivan says, “looks like nothing here”
- Andrei says, “we’ll see, How big is the file system and how big is the device?”

Getting Ready to Look

- Don’t just look at the data:
  - Might make a change to the data or meta-data
  - Device might fail during repeated use
  - Work from a copy
- The first step was create an exact copy of the flash drive **without making any changes to the original**
- A cryptographic hash is computed and used to verify the integrity of acquired data. (re-compute the hash to verify that nothing has been changed.)
- Could be an actual copy or an *image* of ALL DATA on the original.

Cryptographic Hash Function

- Takes a variable length (1 byte to more that 1 TB) and computes a fixed length *hash value*.
- Hashes are unique with a small (really really small) chance the two files have the same hash value by chance.
- The National Software Reference Library (NSRL) at NIST has the goal of hashing every legal file in every application in the known universe (no porn).
- The NSRL can be used to classify files as “known to be installed” or “file might be user created”
- The verb “to de-NIST” means to remove known files from consideration, often seen in civil litigation.

File Systems Timeout

- Keep Plato’s Allegory of the Cave in mind: http://en.wikipedia.org/wiki/Allegory_of_the_Cave
- What seems to be reality may just be a shadow.
- In this case, what the computer user can see is just the data in allocated files. This is not all the story:
  - A storage device is *partitioned* into one or more *file systems*
  - There is unallocated space, i.e., place to put new files or content of deleted files
  - Meta-data describes allocated data, and file systems on device
- All device contents are potentially useful, not just file contents.

Looking Deeper

- Sasha uses several forensic tools to take a closer look at the data.
- She creates a *new case* and adds the image of Nick's flash drive
- They notice an anomaly: The file system is 16MB, but the device is 32MB
- Could be nothing, or could be something hidden
- Let's try *File Carving*

File System Layout Timeout

- To a computer user, a file looks like a continuous stream of bytes, one after another. But this is just a shadow of the reality.
- The reality is that a storage device is divided into partitions, formatted as a file system: FAT, ExFAT, NTFS, HSF+, Ext, . . .
- The file is split into equal size chunks (called clusters or blocks) that can placed anywhere space can be found.
- For a given file system the chunk size is a multiple of 512 bytes
- File meta-data tracks location and sequence of the chunks.
- However, the chunks are often laid out contiguously & in order

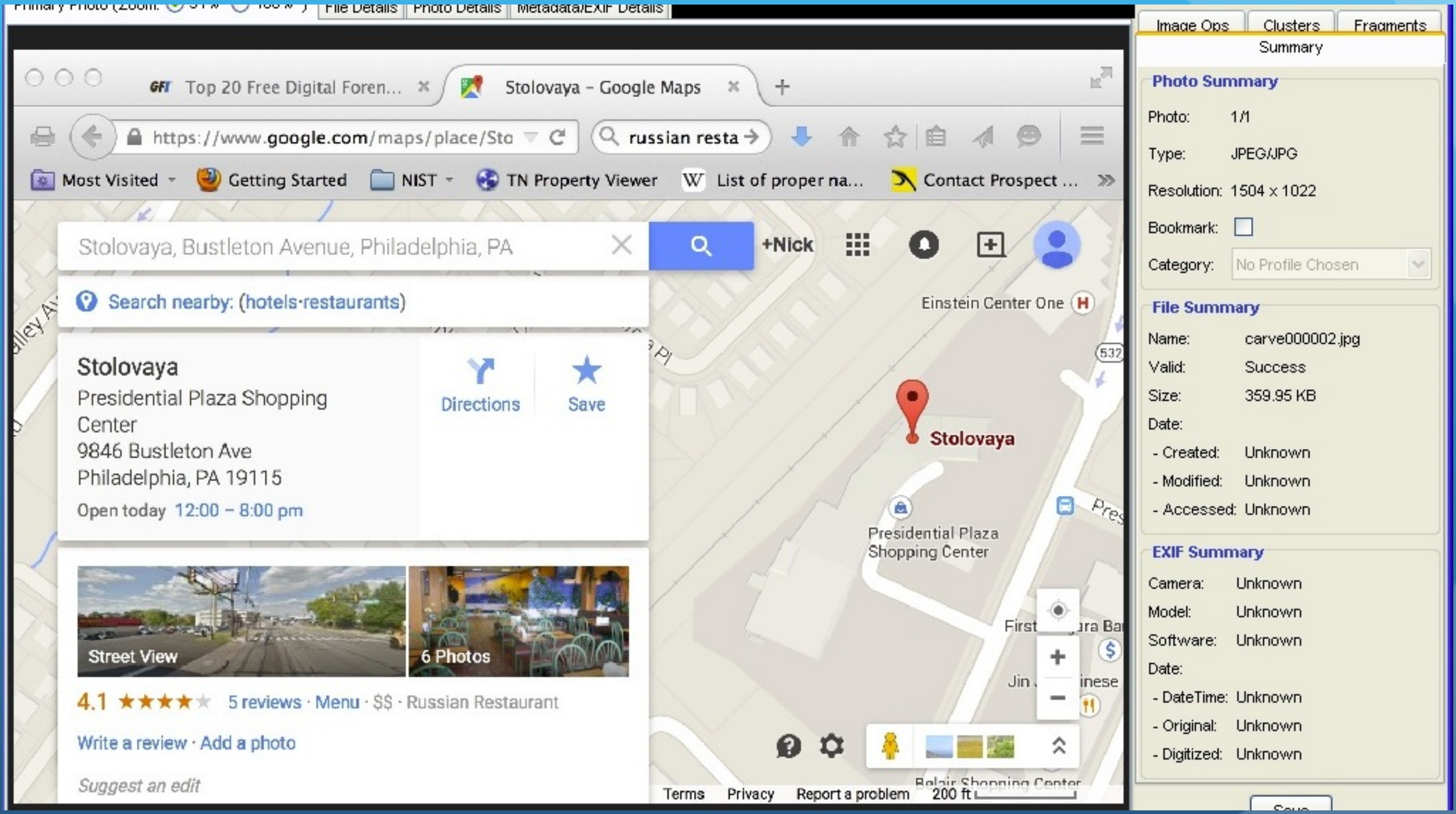
File Types

- There are lots of different file types: pictures, audio, video, document, spreadsheet, data-base, etc.
- These file types are often highly structured.
- These structures can often be recognized and decoded
- If fact, files often have a *magic number* in the first few bytes of a file that identifies the file type
- Some files, e.g., JPG pictures often have lots of meta-data about the picture, e.g., camera, location (GPS) , etc
- So, what can we do . . .

File Carving

- Half of Nick’s flash drive isn’t even part of a file system
- Deleting files and whole file systems is not done by erasing data or even all meta-data. Just mark the object as deleted and available for reuse
- Nick may have just deleted a second file system.
- Data & meta-data are still there, just not visible
- Sasha tries a file carving tool to the unallocated space and . . .

Carving Tool



Stolovaya, Bustleton Avenue, Philadelphia, PA

Search nearby: (hotels·restaurants)

Stolovaya
Presidential Plaza Shopping Center
9846 Bustleton Ave
Philadelphia, PA 19115
Open today 12:00 – 8:00 pm

4.1 ★★★★☆ 5 reviews · Menu · $$ · Russian Restaurant

Write a review · Add a photo

Suggest an edit

Photo Summary

Photo: 1/1
Type: JPEG/JPG
Resolution: 1504 x 1022
Bookmark: □
Category: No Profile Chosen

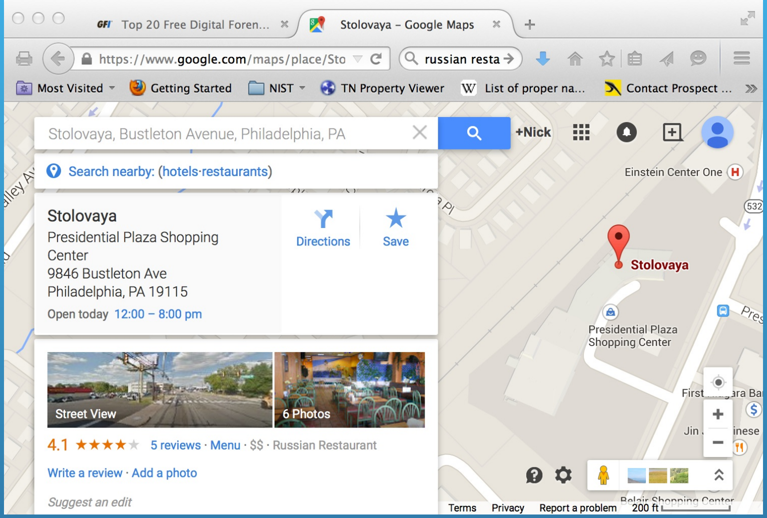
File Summary

Name: carve000002.jpg
Valid: Success
Size: 359.95 KB
Date:
- Created: Unknown
- Modified: Unknown
- Accessed: Unknown

EXIF Summary

Camera: Unknown
Model: Unknown
Software: Unknown
Date:
- DateTime: Unknown
- Original: Unknown
- Digitized: Unknown

Carving Results



Stolovaya, Bustleton Avenue, Philadelphia, PA

Search nearby: (hotels·restaurants)

Stolovaya
Presidential Plaza Shopping Center
9846 Bustleton Ave
Philadelphia, PA 19115

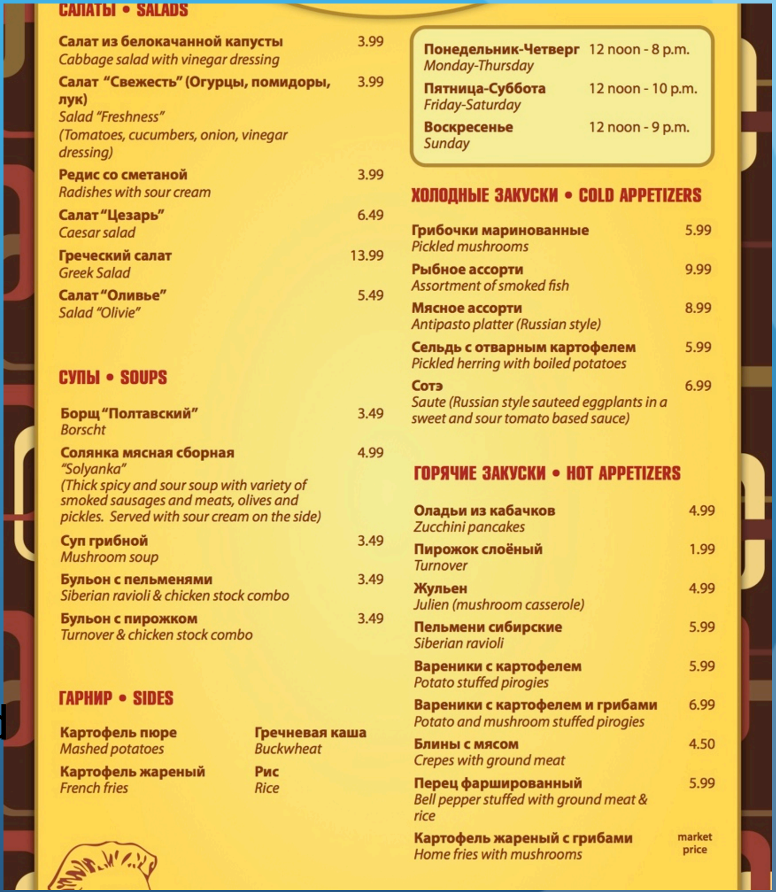
Open today 12:00 – 8:00 pm

4.1 ★★★★☆ 5 reviews · Menu · $$ · Russian Restaurant

Write a review · Add a photo

Suggest an edit

- Surprise! Not Natasha’s Menu
- May be relevant – Nick is interested in Russian Restaurant Menus



САЛАТЫ • SALADS

Салат из белокачанной капусты *Cabbage salad with vinegar dressing*	3.99
Салат “Свежесть” (Огурцы, помидоры, лук) *Salad “Freshness”* *(Tomatoes, cucumbers, onion, vinegar dressing)*	3.99
Редис со сметаной *Radishes with sour cream*	3.99
Салат “Цезарь” *Caesar salad*	6.49
Греческий салат *Greek Salad*	13.99
Салат “Оливье” *Salad “Olivie”*	5.49

СУПЫ • SOUPS

Борщ “Полтавский” *Borscht*	3.49
Солянка мясная сборная *“Solyanka”* *(Thick spicy and sour soup with variety of smoked sausages and meats, olives and pickles. Served with sour cream on the side)*	4.99
Суп грибной *Mushroom soup*	3.49
Бульон с пельменями *Siberian ravioli & chicken stock combo*	3.49
Бульон с пирожком *Turnover & chicken stock combo*	3.49

ГАРНИР • SIDES

Картофель пюре
Mashed potatoes

Картофель жареный
French fries

Гречневая каша
Buckwheat

Рис
Rice

Понедельник-Четверг *Monday-Thursday*	12 noon - 8 p.m.
Пятница-Суббота *Friday-Saturday*	12 noon - 10 p.m.
Воскресенье *Sunday*	12 noon - 9 p.m.

ХОЛОДНЫЕ ЗАКУСКИ • COLD APPETIZERS

Грибочки маринованные *Pickled mushrooms*	5.99
Рыбное ассорти *Assortment of smoked fish*	9.99
Мясное ассорти *Antipasto platter (Russian style)*	8.99
Сельдь с отварным картофелем *Pickled herring with boiled potatoes*	5.99
Сотэ *Saute (Russian style sauteed eggplants in a sweet and sour tomato based sauce)*	6.99

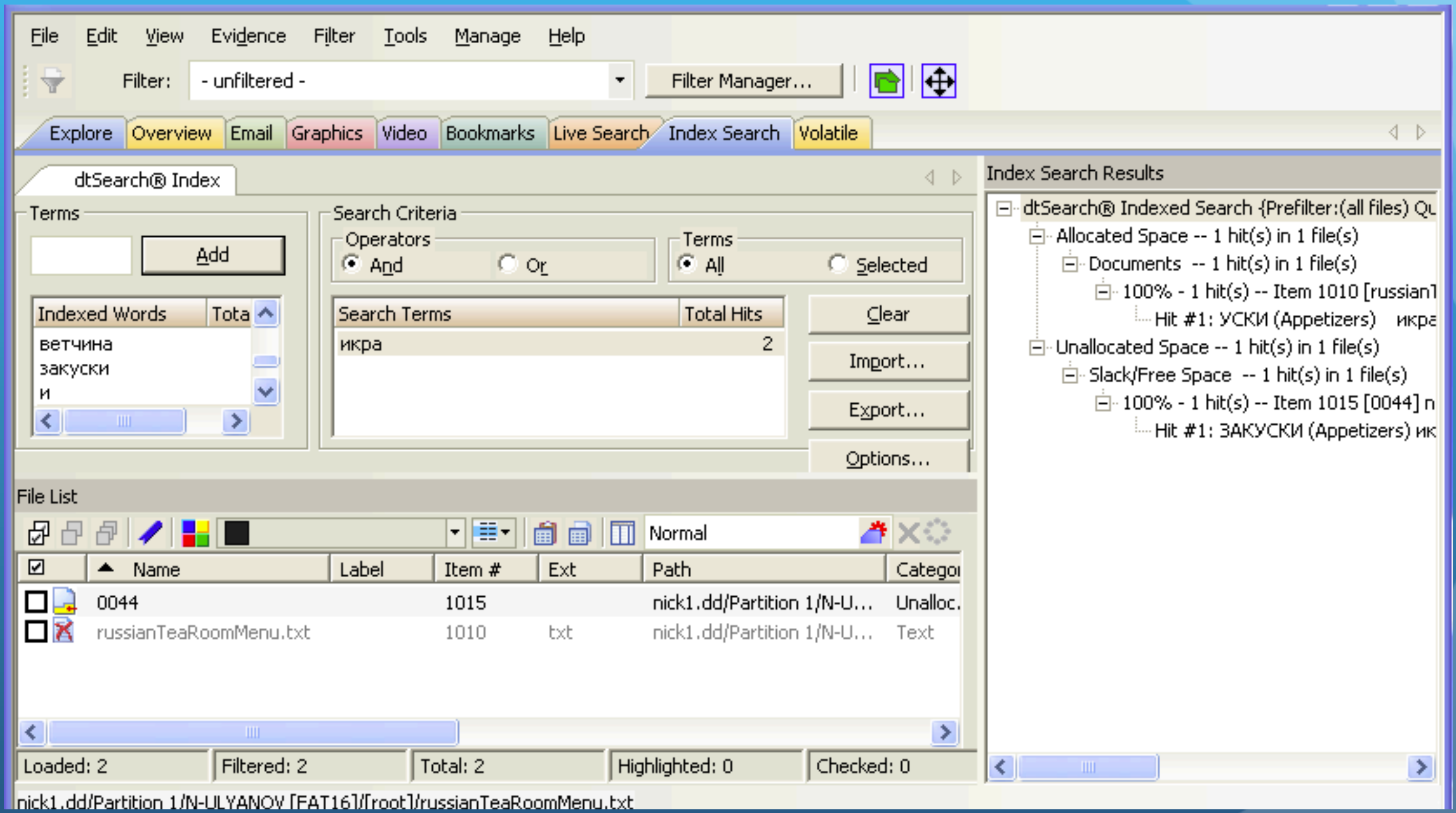
ГОРЯЧИЕ ЗАКУСКИ • HOT APPETIZERS

Оладьи из кабачков *Zucchini pancakes*	4.99
Пирожок слоёный *Turnover*	1.99
Жульен *Julien (mushroom casserole)*	4.99
Пельмени сибирские *Siberian ravioli*	5.99
Вареники с картофелем *Potato stuffed pirogies*	5.99
Вареники с картофелем и грибами *Potato and mushroom stuffed pirogies*	6.99
Блины с мясом *Crepes with ground meat*	4.50
Перец фаршированный *Bell pepper stuffed with ground meat & rice*	5.99
Картофель жареный с грибами *Home fries with mushrooms*	market price

Caviar Anyone?

- Andrew asks Natasha for some menu items that could be searched for.
- He uses another tool and does a string search search for “икра” (Caviar)
- The tool returns a hit not located within an allocated file: икра............................. caviar
- Looks like Nick may have deleted a text file with a menu.
- Andrew does a *Recover deleted files* from the active file system

Where is “икра” (Caviar)?



Filter: - unfiltered -

Operators: ● And ○ Or

Terms: ● All ○ Selected

Indexed Words	Tota
ветчина	
закуски	
и	

Search Terms	Total Hits
икра	2

```
dtSearch® Indexed Search {Prefilter:(all files) Qu
  Allocated Space -- 1 hit(s) in 1 file(s)
    Documents -- 1 hit(s) in 1 file(s)
      100% - 1 hit(s) -- Item 1010 [russianT
        Hit #1: УСКИ (Appetizers)   икра
  Unallocated Space -- 1 hit(s) in 1 file(s)
    Slack/Free Space -- 1 hit(s) in 1 file(s)
      100% - 1 hit(s) -- Item 1015 [0044] n
        Hit #1: ЗАКУСКИ (Appetizers) ик
```

Normal

☑	Name	Label	Item #	Ext	Path	Categoi
□	0044		1015		nick1.dd/Partition 1/N-U...	Unalloc.
□	russianTeaRoomMenu.txt		1010	txt	nick1.dd/Partition 1/N-U...	Text

Loaded: 2 | Filtered: 2 | Total: 2 | Highlighted: 0 | Checked: 0

nick1.dd/Partition 1/N-ULYANOV [FAT16]/[root]/russianTeaRoomMenu.txt

Number Symbols

0	1	2	3	4	5	6	7	8	9
٠	١	٢	٣	٤	٥	٦	٧	٨	٩
零	一	二	三	四	五	六	七	八	九

- Numbers are written as strings of symbols – 10 symbols – base 10
- In Babylon base 60 was used, we still use base 60 in time and geometry
- Computers use two symbols: 0,1 -- binary

Computer Numbers – finite size

- Finite size, e.g. 3 bits (Normally 32 or 64 bit)
- Only positive numbers, consider the biggest numbers negative!!! Math term: modular arithmetic

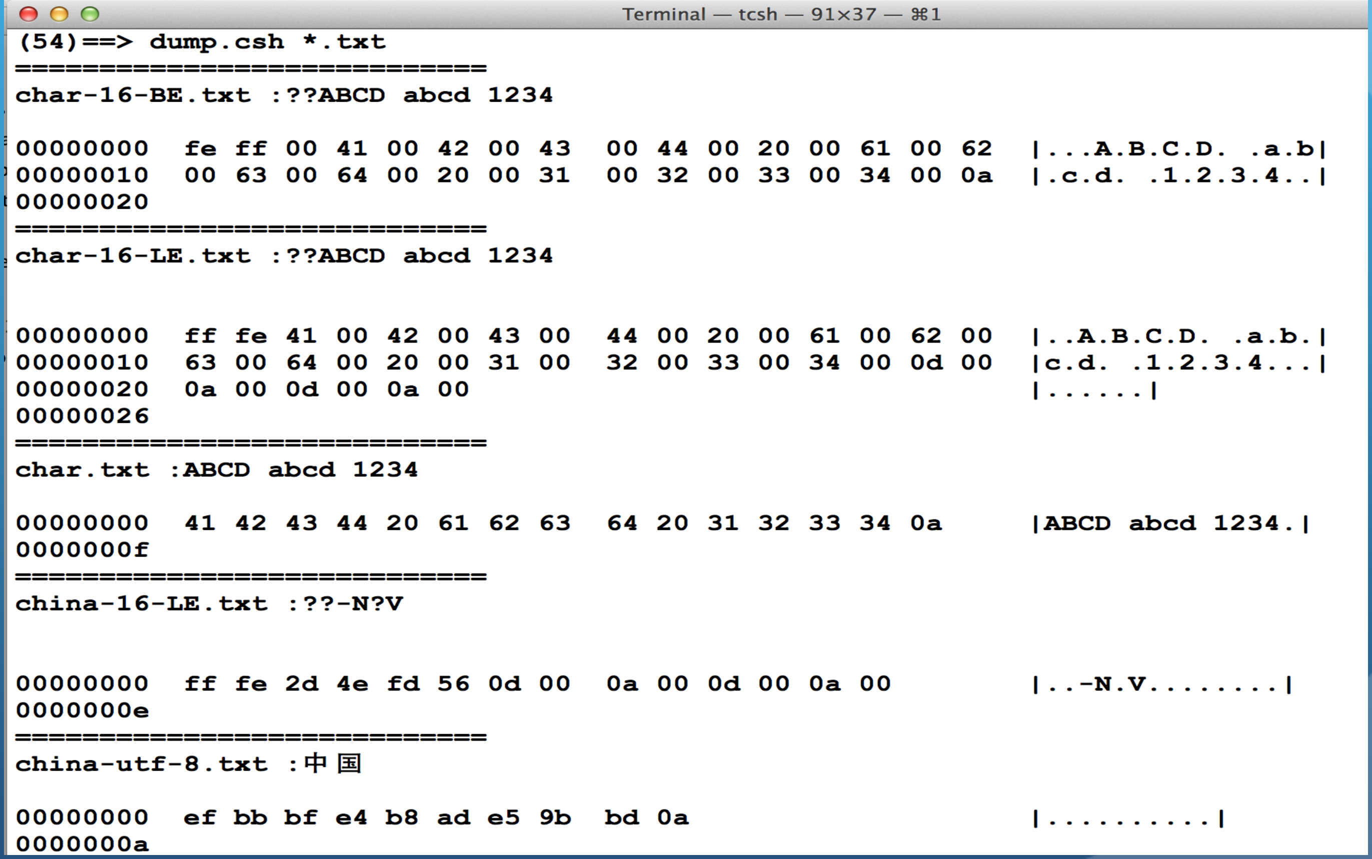
0	000	0
1	001	1
2	010	2
3	011	3
4	100	-4
5	101	-3
6	110	-2
7	111	-1

What about Text?

- Computers use numbers for text
- Each Character (i.e., a-z) is assigned a number (more than one way to do it)
- How big for English? 26 letters, 2 cases, 10 digits & some punctuation – 128 ASCII Characters
- Wait, I need tilde (ñ) and umlaut (ö) – 256 extended ASCII
- And Arabic (الكباب)
- 256 Alternate ISO/IEEE 8859
- Did I mention – 中國 Chinese & Japanese need thousands
- UNICODE 16/32 bit char & variable length UTF-8

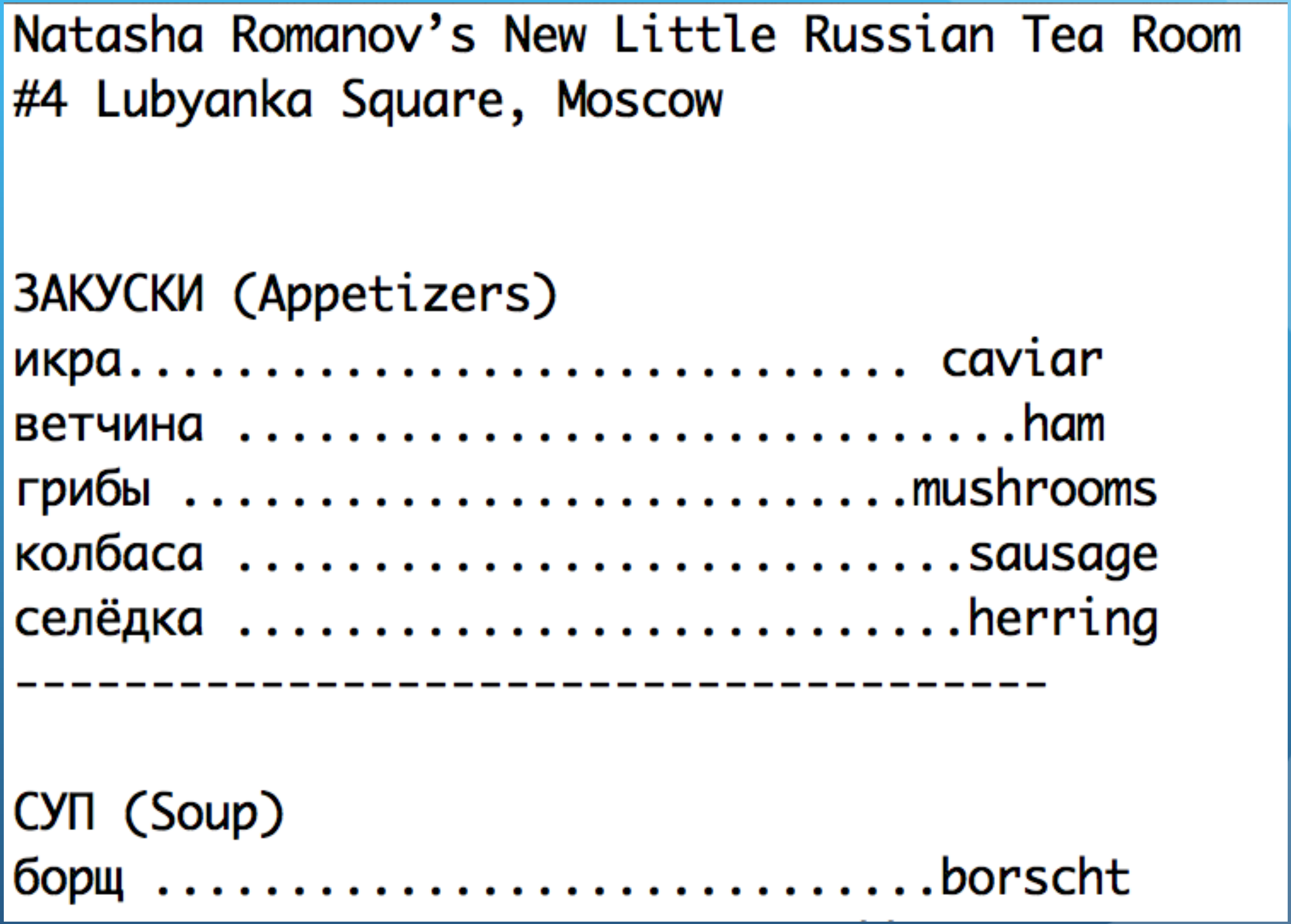
Characters

- Many possible representations – need to check



```
(54)==> dump.csh *.txt
============================
char-16-BE.txt :??ABCD abcd 1234

00000000  fe ff 00 41 00 42 00 43  00 44 00 20 00 61 00 62  |...A.B.C.D. .a.b|
00000010  00 63 00 64 00 20 00 31  00 32 00 33 00 34 00 0a  |.c.d. .1.2.3.4..|
00000020
============================
char-16-LE.txt :??ABCD abcd 1234


00000000  ff fe 41 00 42 00 43 00  44 00 20 00 61 00 62 00  |..A.B.C.D. .a.b.|
00000010  63 00 64 00 20 00 31 00  32 00 33 00 34 00 0d 00  |c.d. .1.2.3.4...|
00000020  0a 00 0d 00 0a 00                                 |......|
00000026
============================
char.txt :ABCD abcd 1234

00000000  41 42 43 44 20 61 62 63  64 20 31 32 33 34 0a     |ABCD abcd 1234.|
0000000f
============================
china-16-LE.txt :??-N?V


00000000  ff fe 2d 4e fd 56 0d 00  0a 00 0d 00 0a 00        |..-N.V........|
0000000e
============================
china-utf-8.txt :中国

00000000  ef bb bf e4 b8 ad e5 9b  bd 0a                    |..........|
0000000a
```

A Deleted File Recovered



```
Natasha Romanov’s New Little Russian Tea Room
#4 Lubyanka Square, Moscow



ЗАКУСКИ (Appetizers)
икра............................. caviar
ветчина .............................ham
грибы ...........................mushrooms
колбаса ...........................sausage
селёдка ...........................herring
--------------------------------------


СУП (Soup)
борщ .............................borscht
```

“What Have We Done?” asks Ivan.

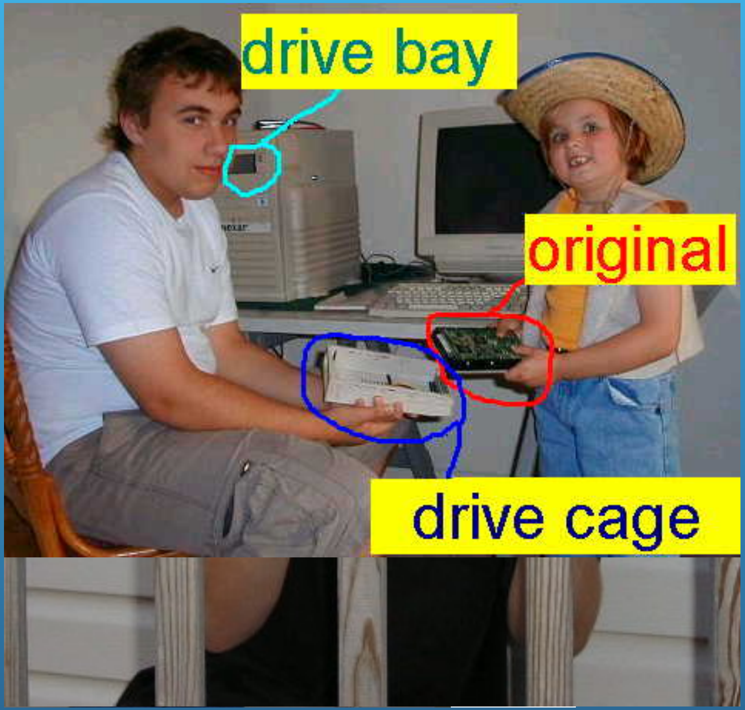
- “Have we shown that Nick is guilty?” asks Ivan
- Sasha & Andrew shake their heads. “No, that’s not what we do.”
- We use our wits and our tools to reveal the truth. If we try to prove the case one way or the other then we fall into the trap of *confirmation bias*. Only finding what we expect.
- Nick may be guilty or not guilty. This is for the case agent and prosecutor to present to the court.
- The court decides.

What Did Ivan Durok Learn?

- Image (make a copy of & hash) evidence without changing it
- Get all data, even from unallocated space
- Work from an image file or copy
- Techniques –
  - cryptographic hash function
  - String search
  - File Carving
  - Deleted file recovery
- Ivan wants to continue study, in America, maybe in Philly (there is a Russian Restaurant there)

An Investigation

- Suspect
- Authorization
- Seize evidence
- Deliver to lab
- Make image
- Analyze
- Report Results



As for Nick . . .

- Found guilty
- Ordered to Siberia
- Appeals for a pardon from the Tsar: “I was framed”
- Ruling: PARDON IMPOSSIBLE, TO BE SENT TO SIBERIA
- Natasha notices her ex-boyfriend, Rasputin the jealous, is unusually cheerful, picks his pocket and takes a quick look at his cell phone and realizes that Nick was framed.
- Natasha intercepts the message ordering Nick away and makes a small change:
- Ruling: PARDON, IMPOSSIBLE TO BE SENT TO SIBERIA

A Shocking Revelation . . .

Computers can be involved in crime …

- As a victim
- As a weapon
- As a witness
- As a record
- As contraband

Agent in the Middle

- When Natasha intercepted and “fixed” the message to send Nick to Siberia she was performing a classic “agent in the middle” attack.
- You think you are connected to your bank/office/friend/etc from the free wi-fi at Panera but someone is monitoring the traffic for:
  - User name/password pairs
  - Account numbers, what else?
- Encryption helps, if there is no “heart bleed” (some flaw in implementation defeating encryption)

Internet Crime

- Phishing
- Ransom ware/Blackmail
- Stealing Data
- Copyright

Intrusion Forensics

- Detection/Identification
- Preserve evidence
- Containment
- Eradication/Attack vector determination
- Damage assessment
- Repair

Where to Find Digital Evidence

- Computer hard drive
- Flash Drive
- Mobile device: phone, tablet, game console, sewing machine, GPS
- Car
- Network traffic
- Router

Extracting Digital Evidence

- Read the binary (not so much now-a-days)
- General purpose tools do a variety of functions
  - String Search
  - File Carve
  - Deleted File Recovery
  - Hashing
- Special tools
  - Mobile Devices
  - File Carving
  - Data acquisition
  - Live memory analysis

Digital Error Rates

- Multiple considerations – Digital Forensics not like many other disciplines with “Is it a match?” questions.
- Technique errors
- Software Implementation errors (not usually a rate)
- Practitioner errors – can a person follow the recipe without messing up

Digital Error Example

- We have carved the Web Page Visit Log and we see:
- 652 visits to Chloroform which could have been used to subdue a murder victim
- (Some data was skipped and not visible, shown as ~~strikethrough~~

Web Page Visit Log				
Page	Xxx	YYY	ZZZ	# visits
Chloroform	DDDDDD	~~DDDDDD~~	~~DDDDD~~	~~1~~
~~Chlorophyll~~	~~DDDDDD~~	~~DDDDDD~~	~~DDDDDD~~	~~345~~
~~Photosynthesis~~	~~DDDDD~~	DDDDD	DDDDD	652

Actual Web Log

- Chloroform looks like an obvious mistyping (autocorrect maybe)
- The data missed in carving just happened to line up in an unfavorable way
- The suspect was doing a homework assignment on Trees

Web Page Visit Log				
Page	Xxx	YYY	ZZZ	# visits
Chloroform	DDDDDD	DDDDDD	DDDDD	1
Chlorophyll	DDDDDD	DDDDDD	DDDDDD	345
Photosynthesis	DDDDD	DDDDD	DDDDD	652

Actual DE Errors

- The DE tools often have quirky behavior, but if the tool user is aware of the behaviors, there isn’t a problem
- The above example is not real, but similar to a real case
- In the real case, the carving tool was not tested enough and was not ready for real use.
- The usual errors are more of the missing something flavor and not of the create something that is not there variety
- When errors happen, it is from improper association

Some Random Bits of History

- 1923 *Frye v. United States* -- expert testimony must be based on scientific methods that are sufficiently established and accepted
- 1993 Daubert – FRE-702 Judge is gate keeper for expert testimony: tested/error rates/peer review/generally accepted/standards & controls
- 2004 Madrid -- Brandon Mayfield has fingerprints similar to Ouhnane Daoud
- 2009 NAS Report – Forensic science needs overhaul

Scientific Working Groups

- Since the early 1990s, American and International forensic science laboratories and practitioners have collaborated in **Scientific Working Groups** (SWGs) to improve discipline practices and build consensus standards.
    - SWGDAM - DNA Analysis
    - SWGDE - Digital Evidence
    - SWGDOC - Questioned Documents
    - SWGDOG - Dogs and Orthogonal Detection
    - SWGWILD – Wildlife Forensics
    - SWGFAST - Latent Fingerprints
- In 2014, the SWGs are being reorganized under the NIST Organization for Scientific Area Committees (OSAC)

Some Resources

- SWGDE www.swgde.org
- OSAC-DE www.nist.gov/forensics/osac/sub-de.cfm
- AAFS http://www.aafs.org/
- DFRWS http://www.dfrws.org/
- SANS www.sans.org/
- 洗冤集錄 ***Washing Away of Wrongs*** ***http://en.wikipedia.org/wiki/Collected_Cases_of_Injustice_Rectified***
- Poisoner's Handbook see Amazon.com

That's All

- Questions?
- Jim Lyle – JLYLE@NIST.GOV