cyber discovery camp

SPONSORED BY

Louisiana Tech University
and Cyber Innovation Center


CYBER
DISCOVERY
→ Hard Drive Analysis
→ Investigating a Crime Scene
→ Basic Cryptography
INVESTIGATIVE SESSION 2

Hard Drive Analysis

- Hard drive investigation or hard drive analysis is one aspect of a larger field of work called Digital Forensics
- Digital Forensics is forensics applied to information stored or transported on digital devices
  - These include computers, cell phones, tablets, etc

CYBER DISCOVERY

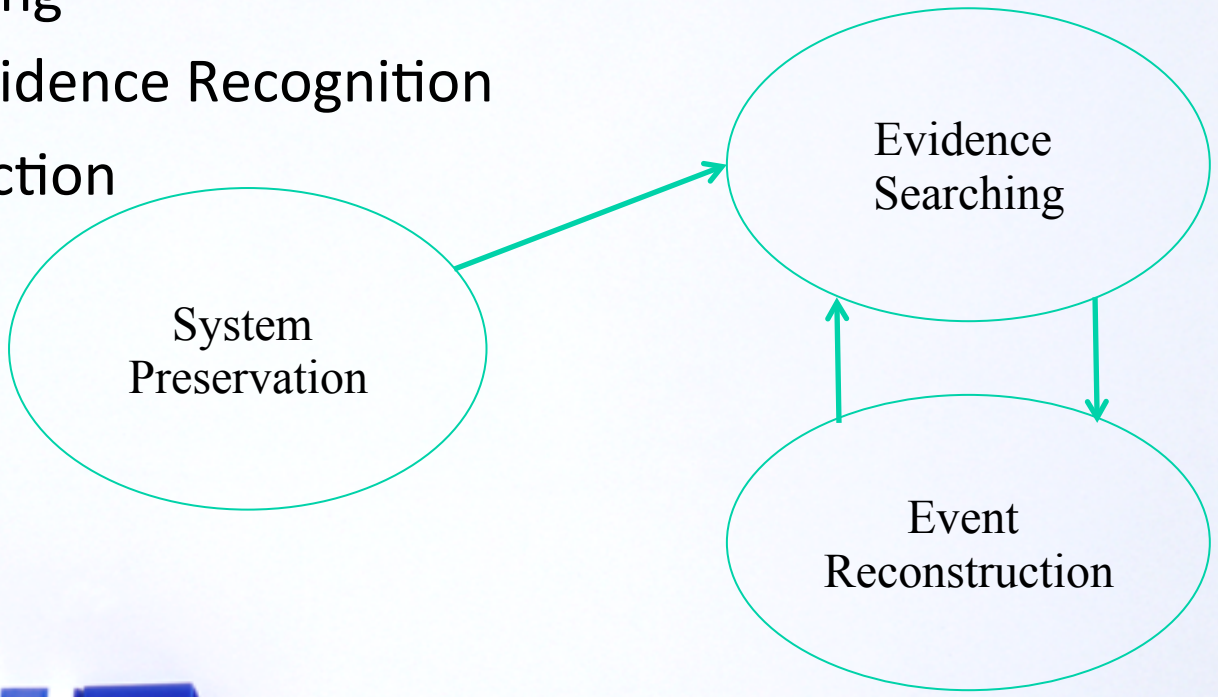
Three Phases

- Digital Forensics has three main phases
  - System Preservation
  - Evidence Searching
    - Also called Evidence Recognition
  - Event Reconstruction

CYBER DISCOVERY

Three Phases

- Digital Forensics has three main phases
  - System Preservation
  - Evidence Searching
    - Also called Evidence Recognition
  - Event Reconstruction



System Preservation

- System preservation is just as it sounds, we are preserving the system
  - Reduce or limit the amount of evidence that may be overwritten
  - We make a copy or an image of the storage media of the digital device (i.e. hard drive)
    - This image is an exact bit-by-bit copy of the original data
    - A special device called a write blocker is used
      - This ensures that the original data is not disturbed

CYBER DISCOVERY

System Preservation

- This raises a question.
- Why can't we just copy and paste?
- When you access a file, as in copying it, the operating system takes note of that and modifies the metadata (data about data) for that file

CYBER DISCOVERY

Evidence Recognition and Event Reconstruction

- Evidence recognition and event reconstruction are cyclic in nature
  - Like putting a puzzle together
  - First you have to find the correct pieces in a sea of puzzle pieces

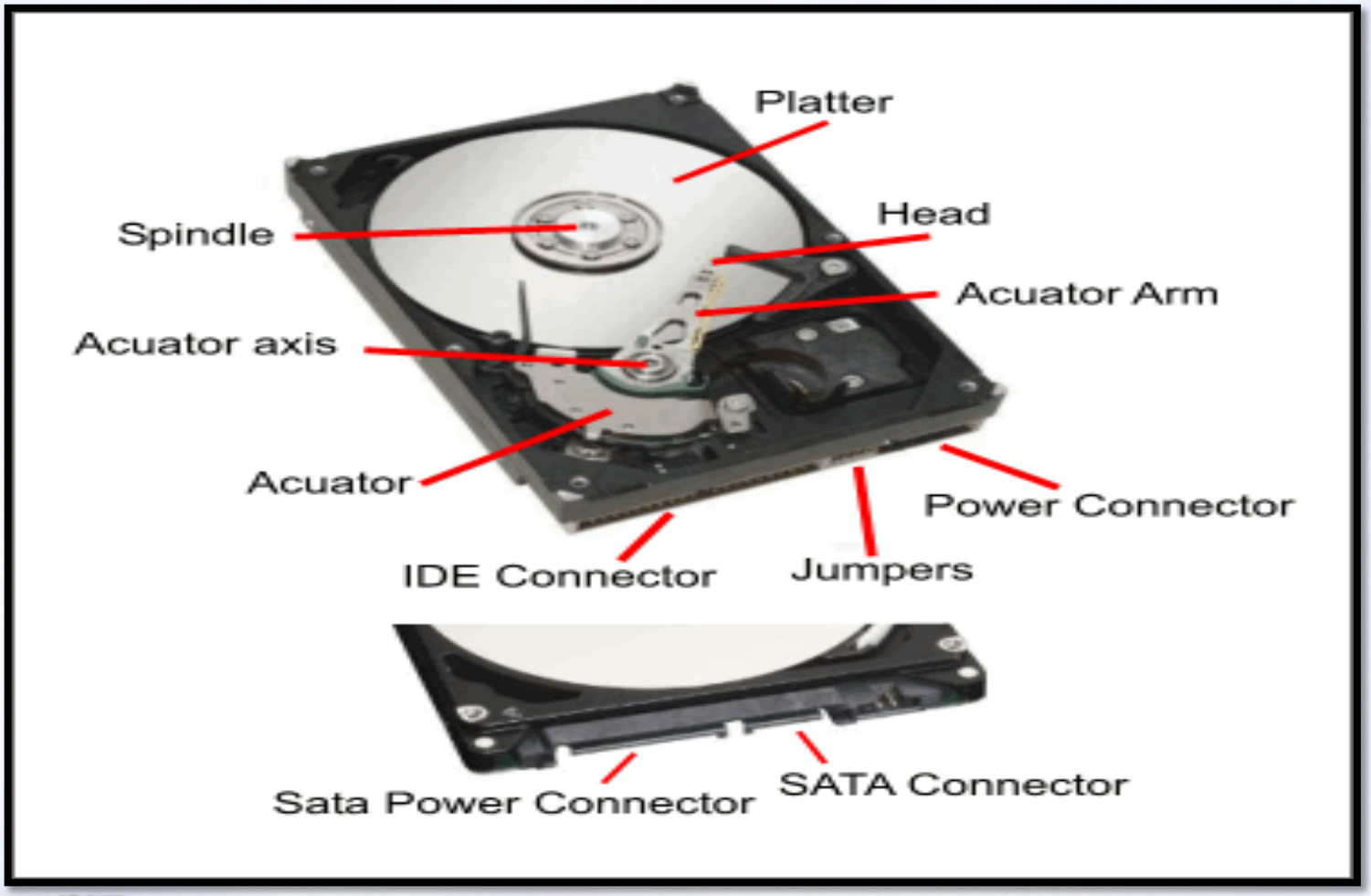
CYBER DISCOVERY

Hard Drives

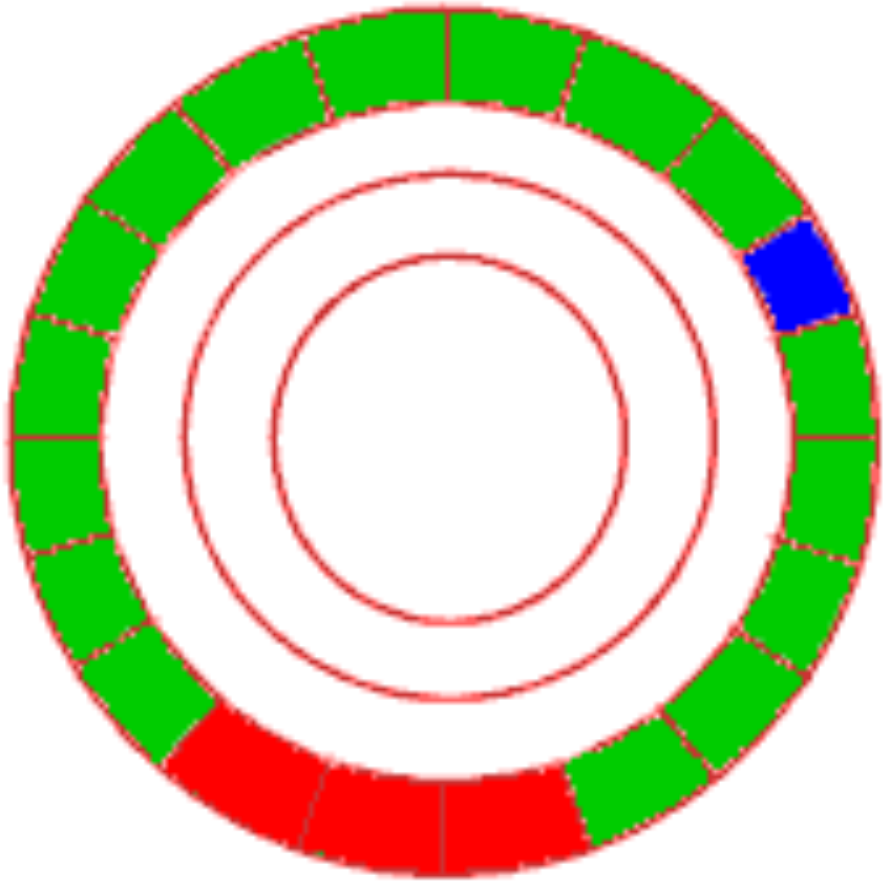
- How are files stored on a hard drive?
  - Physical make-up of a hard drive
    - Disk has several platters in it
      - The platters are where the information is written
      - Platters are divided up into tracks and further into sectors
        - Sectors are usually 512 bytes in size
    - Combine several sectors together and you get a cluster
      - Cluster is the minimum file allocation unit

CYBER DISCOVERY

Hard Drive



Hard Drive



Track

Sector

Cluster

CYBER DISCOVERY

Solid State Drives

- Solid State Drives pose an interesting challenge in digital forensics
- Magnetic drives are very well understood
  - Protocols are standardized
  - With SSDs, many manufactures, many internal protocols

CYBER DISCOVERY

Solid State Drives

- All writes occur on a block-by-block basis
  - Failure possible at 100,000 block writes
- To extent life, device uses a pool of ‘ready to write’ blocks
  - Writes to the block that is least used
- Wear Leveling
  - Once SSD knows that block no longer needed
  - At free time can erase it and move it to pool

CYBER DISCOVERY

Solid State Drives

- Lastly, TRIM function
- Big problem for forensics investigators
- TRIM function allows operating system to inform SSD that an area is no longer needed
  - For example, a file as been deleted
  - Makes recovering deleted files near impossible

CYBER DISCOVERY

Hard Drives

- How are files stored on a hard drive?
  - Now let's discuss how an operating system, like Windows, handles files
    - When you create a file and save it to your hard drive
      - Windows finds enough clusters to store the file and writes it
      - Windows also creates an entry in a lookup table
        - Called the File Allocation Table or Master File Table
          - Depending on the version of Windows
        - This lookup table contains information about your file
          - This is known as metadata
            - Name, size, cluster location, etc

CYBER DISCOVERY

- Tying this back in with ‘why we can’t just copy and paste’
  - We could miss valuable information

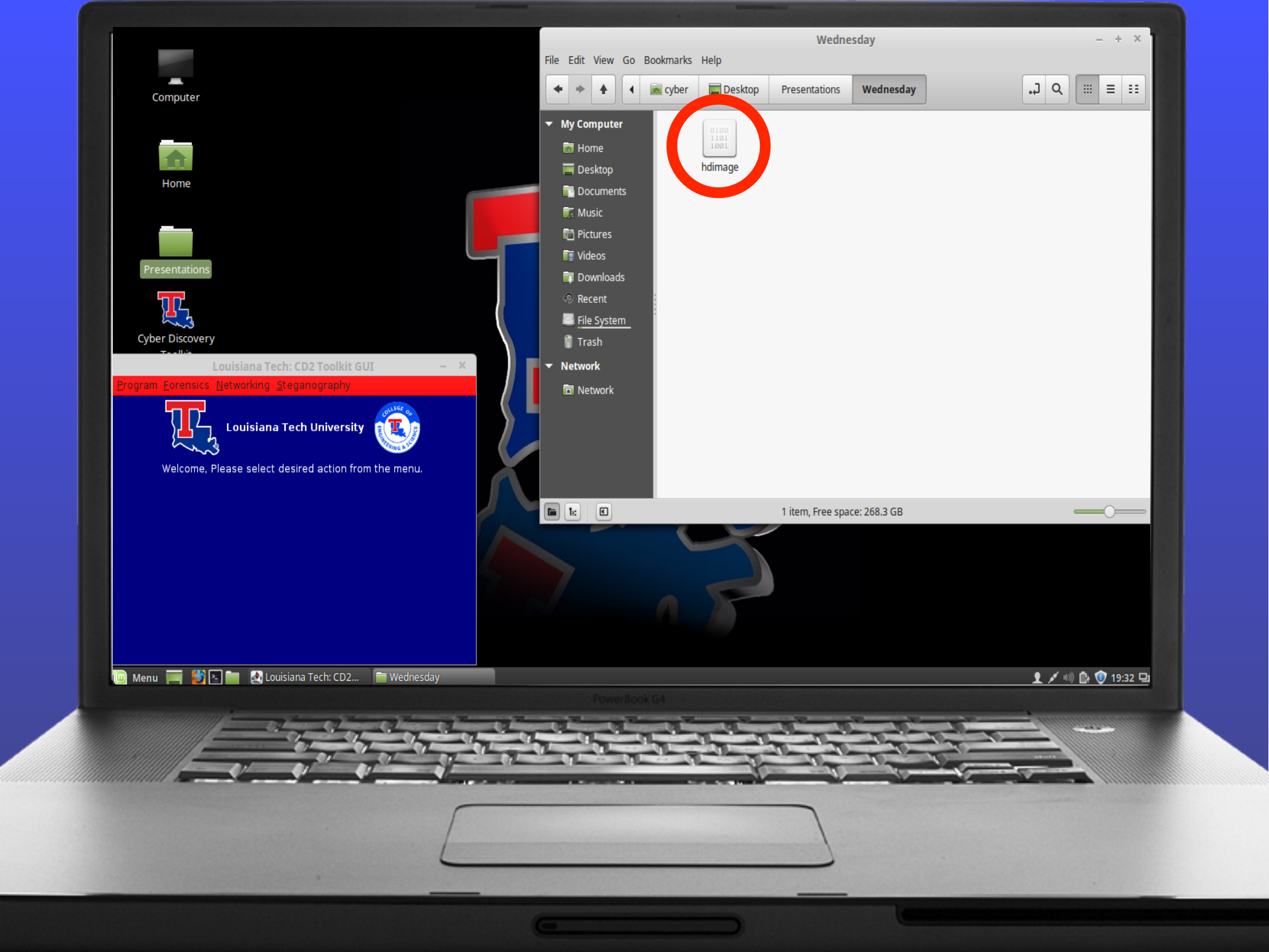
Hands-on

- Let's take a look at the files listed in a given disk image
- We will be using tools within the Cyber Discovery Toolkit called SluethKit

CYBER DISCOVERY

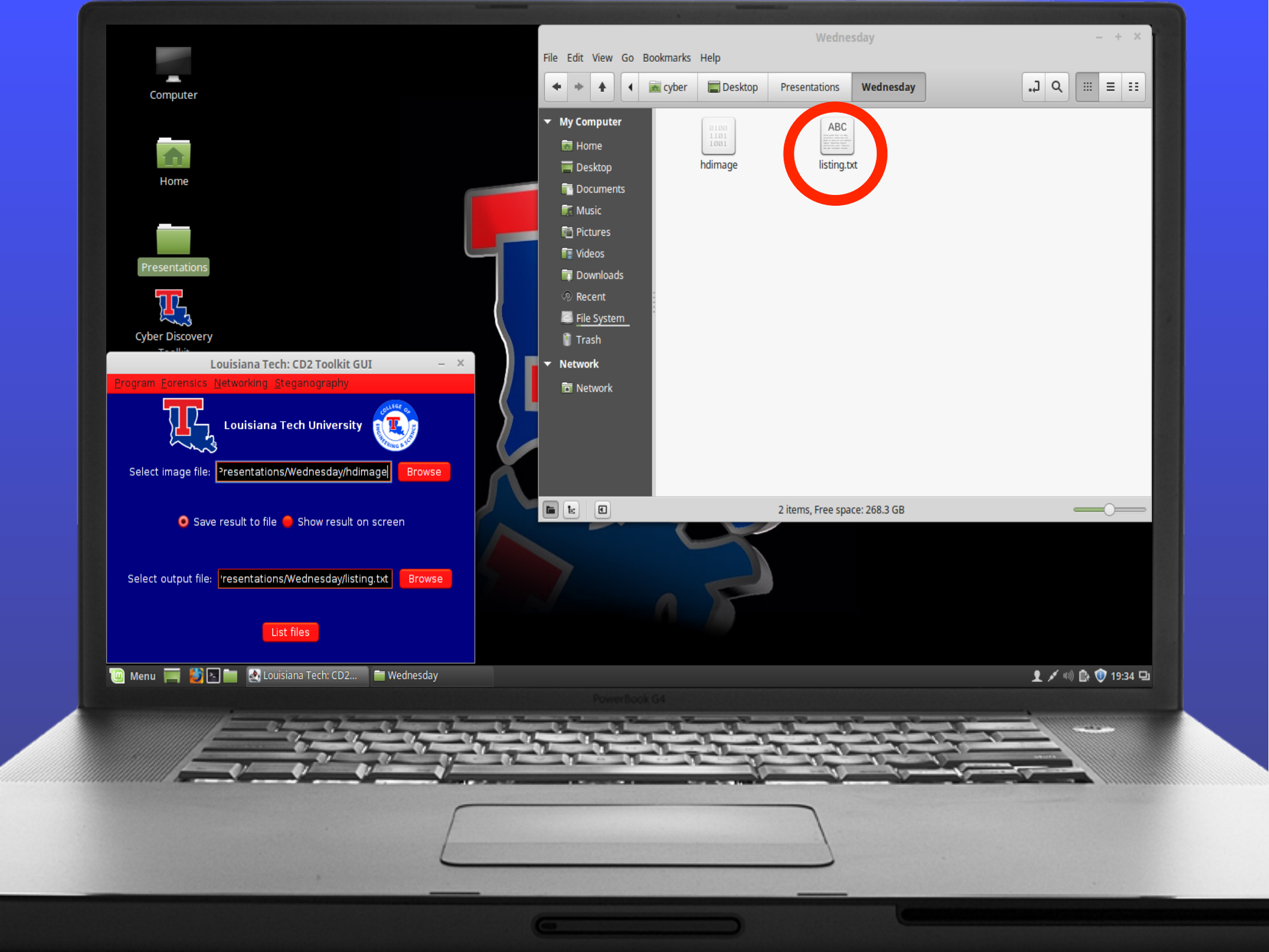

Computer
Home
Presentations
Cyber Discovery Toolkit
Menu
19:32


Computer
Home
Presentations
Cyber Discovery
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Welcome, Please select desired action from the menu.
Menu
Louisiana Tech: CD2...
19:32


Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
1 item, Free space: 268.3 GB
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Welcome, Please select desired action from the menu.
Menu
Louisiana Tech: CD2...
Wednesday
19:32


Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
hdimage
Result
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-1: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
+ r/r 25-144-5: $ObjId:$O
+ r/r 24-144-3: $Quota:$O
+ r/r 24-144-2: $Quota:$Q
+ r/r 26-144-2: $Reparse:$R
r/r 2-128-1: $LogFile
r/r 0-128-1: $MFT
r/r 1-128-1: $MFTMirr
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 3-128-3: $Volume
r/r 7517-128-1: AUTOEXEC.BAT
r/r 3545-128-3: boot.ini
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: ?resentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
Working...
Menu
Louisiana Tech: CD2...
Wednesday
19:33


Computer
Home
Presentations
Cyber Discovery
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file:
Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
resentations/Wednesday/listing.txt
Browse
List files
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
1 item, Free space: 268.3 GB
Menu
Louisiana Tech: CD2...
Wednesday
19:34


Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
ABC
listing.txt
2 items, Free space: 268.3 GB
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file:
Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
resentations/Wednesday/listing.txt
Browse
List files
Menu
Louisiana Tech: CD2...
Wednesday
19:34


Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-1: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
+ r/r 25-144-5: $ObjId:$O
+ r/r 24-144-3: $Quota:$O
+ r/r 24-144-2: $Quota:$Q
+ r/r 26-144-2: $Reparse:$R
r/r 2-128-1: $LogFile
r/r 0-128-1: $MFT
r/r 1-128-1: $MFTMirr
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 3-128-3: $Volume
r/r 7517-128-1: AUTOEXEC.BAT
r/r 3545-128-3: boot.ini
r/r 7516-128-1: CONFIG.SYS
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file:
Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
resentations/Wednesday/listing.txt
Browse
List files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:34


Find
Search for:
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
r/r 4-128-4: $AttrDef
r/r 8-128-2: $BadClus
r/r 8-128-1: $BadClus:$Bad
r/r 6-128-1: $Bitmap
r/r 7-128-1: $Boot
d/d 11-144-4: $Extend
+ r/r 25-144-5: $ObjId:$O
+ r/r 24-144-3: $Quota:$O
+ r/r 24-144-2: $Quota:$Q
+ r/r 26-144-2: $Reparse:$R
r/r 2-128-1: $LogFile
r/r 0-128-1: $MFT
r/r 1-128-1: $MFTMirr
r/r 9-128-8: $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-14: $Secure:$SII
r/r 10-128-1: $UpCase
r/r 3-128-3: $Volume
r/r 7517-128-1: AUTOEXEC.BAT
r/r 3545-128-3: boot.ini
r/r 7516-128-1: CONFIG.SYS
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file:
Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
resentations/Wednesday/listing.txt
Browse
List files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:34


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
+++ r/r 13949-128-4: Cell.pdf:Zone.Identifier
+++ r/r 13588-128-1: Charles.txt
+++ r/r 10733-128-4: Copy (2) of Italia.jpg
+++ r/r 10734-128-4: Copy (3) of Italia.jpg
+++ r/r 10732-128-4: Copy of Italia.jpg
+++ r/r 13883-128-3: DIGI_for.pdf
+++ r/r 13883-128-4: DIGI_for.pdf:Zone.Identifier
+++ r/r 12997-128-3: Doggies.jpg
+++ r/r 12609-128-1: Explanation.txt
+++ r/r 12573-128-3: Frisbee.jpg
+++ r/r 12941-128-1: Fun_Riddle.txt
+++ r/r 13947-128-4: Happy_or_Sad.pdf
+++ r/r 13947-128-5: Happy_or_Sad.pdf:Zone.Identifier
+++ r/r 10717-128-3: Italia.jpg
+++ r/r 12736-128-3: Messi.jpg
+++ d/d 10453-144-7: MyThings
++++ d/d 10585-144-6: 2011-2012
+++++ d/- * 0: Bob Crane
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 629, Col 35
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: resentations/Wednesday/listing.txt
Browse
List files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:36

Hard Drive Analysis

```
+++ r/r 10717-128-3:     Italia.jpg
```

- What do the values in front of the filename mean?
- The + signs provide for the depth in the directory structure
- The `r/r` provides the file type
  - `r/r` means that this is a file
  - `d/d` means that this is a directory
- The number is the metadata address or `inode` number

CYBER DISCOVERY


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
hdimage
listing.txt
Result
MFT Entry Header Values:
Entry: 10717 Sequence: 7
$LogFile Sequence Number: 42894539
Allocated File
Links: 1
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 359 (S-1-5-21-1177238915-1343024091-1435490099-1003)
Created: 2015-07-15 17:47:05 (CDT)
File Modified: 2015-07-15 17:47:05 (CDT)
MFT Modified: 2015-07-15 17:47:10 (CDT)
Accessed: 2015-07-16 04:22:26 (CDT)
$FILE_NAME Attribute Values:
Flags: Archive
Name: Italia.jpg
Parent MFT Entry: 10397 Sequence: 1
Allocated Size: 0 Actual Size: 0
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10717-128-3
Working...
++++ d/d 10585-144-6: 2011-2012
+++++ d/- * 0: Bob Crane
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 629, Col 35
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:37


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
hdimage
listing.txt
Result
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-2) Name: N/A Resident size: 86
Type: $OBJECT_ID (64-4) Name: N/A Resident size: 16
Type: $DATA (128-3) Name: N/A Non-Resident size: 719397 init_size: 719397
1125687 1125688 1125689 1125690 1125691 1125692 1125693 1125694
1155594 1155595 1155596 1155597 1155598 1155599 1155600 1155601
1155602 1155603 1155604 1155605 1155606 1155607 1155608 1155609
1219229 1219230 1219231 1219232 1219233 1219234 1219235 1219236
1219237 1219238 1219239 1219240 1219241 1219242 1219243 1219244
1219245 1219246 1219247 1219248 1219249 1219250 1219251 1219252
1219253 1219254 1219255 1219256 1219257 1219258 1219259 1219260
48757 48758 48759 48760 48761 48762 48763 48764
48765 48766 48767 48768 48769 48770 48771 48772
48773 48774 48775 48776 48777 48778 48779 48780
48781 48782 48783 48784 48785 48786 48787 48788
48789 48790 48791 48792 48793 48794 48795 48796
48797 48798 48799 48800 48801 48802 48803 48804
48805 48806 48807 48808 48809 48810 48811 48812
48813 48814 48815 48816 48817 48818 48819 48820
48821 48822 94486 94487 94488 94489 94490 94491
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10717-128-3
Working...
++++ d/d 10585-144-6: 2011-2012
+++++ d/- * 0: Bob Crane
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 629, Col 35
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:37


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
Italia.jpg
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
+++ r/r 13949-128-4: Cell.pdf:Zone.Identifier
+++ r/r 13588-128-1: Charles.txt
+++ r/r 10733-128-4: Copy (2) of Italia.jpg
+++ r/r 10734-128-4: Copy (3) of Italia.jpg
+++ r/r 10732-128-4: Copy of Italia.jpg
+++ r/r 13883-128-3: DIGI_for.pdf
+++ r/r 13883-128-4: DIGI_for.pdf:Zone.Identifier
+++ r/r 12997-128-3: Doggies.jpg
+++ r/r 12609-128-1: Explanation.txt
+++ r/r 12573-128-3: Frisbee.jpg
+++ r/r 12941-128-1: Fun_Riddle.txt
+++ r/r 13947-128-4: Happy_or_Sad.pdf
+++ r/r 13947-128-5: Happy_or_Sad.pdf:Zone.Identifier
+++ r/r 10717-128-3: Italia.jpg
+++ r/r 12736-128-3: Messi.jpg
+++ d/d 10453-144-7: MyThings
++++ d/d 10585-144-6: 2011-2012
+++++ d/- * 0: Bob Crane
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 629, Col 35
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: Presentations/Wednesday/Italia.jpg
Browse
iNode number: 10717-128-3
Extract files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:38


Find
Search for:
Italia
Match case
Match entire wo
Search backwar
Wrap around
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
Italia.jpg
Image Edit View Go Help
Previous
Next
1620 × 1080 pixels 719.4 kB 51%
1 / 1
Louisiana Tech: CD2
Program Forensics Networking Stegan
Louisiana Tech U
Select image file:
Presentations/Wedr
Save result to file
Select output file:
Presentations/Wedr
iNode number:
Extract file
ABC
ting.txt
Final Project.docx
- Outline.docx
Plain Text
Tab Width: 8
Ln 629, Col 35
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
Italia.jpg
19:38

Hard Drive Analysis

- Now what about recovering a deleted file?
- In this format deleted files are denoted by an '*' and sometimes the first character of the file name '_'

- Now look at the Dr. Art Final Project.docx file just below

CYBER DISCOVERY


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
Italia.jpg
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
+++ r/r 13949-128-4: Cell.pdf:Zone.Identifier
+++ r/r 13588-128-1: Charles.txt
+++ r/r 10733-128-4: Copy (2) of Italia.jpg
+++ r/r 10734-128-4: Copy (3) of Italia.jpg
+++ r/r 10732-128-4: Copy of Italia.jpg
+++ r/r 13883-128-3: DIGI_for.pdf
+++ r/r 13883-128-4: DIGI_for.pdf:Zone.Identifier
+++ r/r 12997-128-3: Doggies.jpg
+++ r/r 12609-128-1: Explanation.txt
+++ r/r 12573-128-3: Frisbee.jpg
+++ r/r 12941-128-1: Fun_Riddle.txt
+++ r/r 13947-128-4: Happy_or_Sad.pdf
+++ r/r 13947-128-5: Happy_or_Sad.pdf:Zone.Identifier
+++ r/r 10717-128-3: Italia.jpg
+++ r/r 12736-128-3: Messi.jpg
+++ d/d 10453-144-7: MyThings
++++ d/d 10585-144-6: 2011-2012
+++++ d/- * 0: Bob Crane
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 635, Col 67
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: Presentations/Wednesday/Italia.jpg
Browse
iNode number: 10717-128-3
Extract files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:40


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
hdimage
Italia.jpg
listing.txt
Result
MFT Entry Header Values:
Entry: 10607 Sequence: 6
$LogFile Sequence Number: 42650131
Allocated File
Links: 2
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 359 (S-1-5-21-1177238915-1343024091-1435490099-1003)
Created: 2015-07-15 11:25:15 (CDT)
File Modified: 2015-07-15 11:25:15 (CDT)
MFT Modified: 2015-07-15 11:25:15 (CDT)
Accessed: 2015-07-15 11:25:15 (CDT)
$FILE_NAME Attribute Values:
Flags: Archive
Name: Determination of pH- lab.docx
Parent MFT Entry: 10602 Sequence: 4
Allocated Size: 0 Actual Size: 0
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10607-128-4
Working...
Wednesday) - gedit
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 635, Col 67
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:42


Find
Search for: Italia
Match case
Match entire word only
Search backwards
Wrap around
Close
Wednesday
File Edit View Go Bookmarks Help
cyber Desktop Presentations Wednesday
My Computer
Home
Desktop
Documents
Music
hdimage
Italia.jpg
listing.txt
Computer
Home
Presentations
Cyber Discovery
Result
File Modified: 2015-07-15 11:25:15 (CDT)
MFT Modified: 2015-07-15 11:25:15 (CDT)
Accessed: 2015-07-15 11:25:15 (CDT)
$FILE_NAME Attribute Values:
Flags: Archive
Name: Determination of pH- lab.docx
Parent MFT Entry: 10602 Sequence: 4
Allocated Size: 0 Actual Size: 0
Created: 2015-07-15 11:25:15 (CDT)
File Modified: 2015-07-15 11:25:15 (CDT)
MFT Modified: 2015-07-15 11:25:15 (CDT)
Accessed: 2015-07-15 11:25:15 (CDT)
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 90
Type: $FILE_NAME (48-2) Name: N/A Resident size: 124
Type: $DATA (128-4) Name: N/A Non-Resident size: 7788 init_size: 7788
24436 24437
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10607-128-4
Working...
Wednesday) - gedit
+++++ r/- * 0: Dr. Art Final Project.docx
+++++ r/r * 10607-128-4(realloc): Dr. Art Final Project.docx
+++++ r/r * 10633-128-4(realloc): From 992- Outline.docx
Plain Text
Tab Width: 8
Ln 635, Col 67
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:42


Find
Search for: Federal Reserve
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
hdimage
Italia.jpg
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ -/r * 10836-128-3: DSCF3781.JPG
++++++ -/r * 10837-128-4: www.menswearhouse.com.htm
++++++ -/r * 10838-128-3: DSCF3757.JPG
++++++ -/r * 10839-128-4: ScottSports.htm
++++++ -/r * 10840-128-4: Bornstein (an american chron TR).pdf
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
++++++ -/r * 10844-128-4: Classic_models_query.xps
++++++ -/r * 10845-128-3: DSCF3758.JPG
++++++ -/r * 10846-128-3: DSCF3719.JPG
++++++ -/r * 10847-128-4: Federal Reserve Locations.jpg
++++++ -/r * 10848-128-3: DSCF3690.JPG
+++++ r/- * 0: Reading_List.pdf
+++++ -/r * 10736-128-4: Bornstein (an american chron TR).pdf
+++++ -/r * 10849-128-3: Cookbook.pdf
+++ r/r 13950-128-4: Phone_track.pdf
+++ r/r 13950-128-5: Phone_track.pdf:Zone.Identifier
+++ r/r 13604-128-1: Please_read_this.txt
+++ r/r 10696-128-3: pscp.exe
+++ r/r 10696-128-4: pscp.exe:Zone.Identifier
+++ r/r 10690-128-3: putty.exe
Plain Text
Tab Width: 8
Ln 767, Col 62
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10607-128-4
Extract metadata
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:45


Find
Search for: Federal Reserve
Match case
Match entire word only
Search backwards
Wrap around
Close
Wednesday
File Edit View Go Bookmarks Help
cyber Desktop Presentations Wednesday
My Computer
Home
Desktop
Documents
hdimage
Italia.jpg
listing.txt
Result
MFT Entry Header Values:
Entry: 10847 Sequence: 4
$LogFile Sequence Number: 42580144
Not Allocated File
Links: 2
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 359 (S-1-5-21-1177238915-1343024091-1435490099-1003)
Created: 2015-07-15 10:36:13 (CDT)
File Modified: 2015-07-15 10:36:13 (CDT)
MFT Modified: 2015-07-15 10:36:13 (CDT)
Accessed: 2015-07-15 10:36:13 (CDT)
$FILE_NAME Attribute Values:
Flags: Archive
Name: Federal Reserve Locations.jpg
Parent MFT Entry: 10737 Sequence: 3
Allocated Size: 0 Actual Size: 0
OK
Computer
Home
Presentations
Cyber Discovery
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10847-128-4
Working...
+++ r/r 13604-128-1: Please_read_this.txt
+++ r/r 10696-128-3: pscp.exe
+++ r/r 10696-128-4: pscp.exe:Zone.Identifier
+++ r/r 10690-128-3: putty.exe
Plain Text
Tab Width: 8
Ln 767, Col 62
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:46


Find
Search for: Federal Reserve
Match case
Match entire word only
Search backwards
Wrap around
Close
Wednesday
File Edit View Go Bookmarks Help
cyber Desktop Presentations Wednesday
My Computer
Home
Desktop
Documents
hdimage
Italia.jpg
listing.txt
Computer
Home
Presentations
Cyber Discovery
Result
Name: Federal Reserve Locations.jpg
Parent MFT Entry: 10737 Sequence: 3
Allocated Size: 0 Actual Size: 0
Created: 2015-07-15 10:36:13 (CDT)
File Modified: 2015-07-15 10:36:13 (CDT)
MFT Modified: 2015-07-15 10:36:13 (CDT)
Accessed: 2015-07-15 10:36:13 (CDT)
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 90
Type: $FILE_NAME (48-2) Name: N/A Resident size: 124
Type: $DATA (128-4) Name: N/A Non-Resident size: 211693 init_size: 211693
1237354 1237355 1237356 1237357 1237358 1237359 1237360 1237361
1237362 1237363 65482 65483 65484 65485 65486 65487
65488 65489 65490 65491 65492 65493 65494 65495
65496 65497 65498 65499 65500 65501 65502 65503
65504 86478 86479 86480 86481 86482 86483 86484
86485 86486 86487 86488 86489 86490 86491 86492
86493 86494 86495 86496
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10847-128-4
Working...
+++ r/r 13604-128-1: Please_read_this.txt
+++ r/r 10696-128-3: pscp.exe
+++ r/r 10696-128-4: pscp.exe:Zone.Identifier
+++ r/r 10690-128-3: putty.exe
Plain Text
Tab Width: 8
Ln 767, Col 62
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:46


Find
Search for: Federal Reserve
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
Federal.jpg
hdimage
Italia.jpg
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ -/r * 10836-128-3: DSCF3781.JPG
++++++ -/r * 10837-128-4: www.menswearhouse.com.htm
++++++ -/r * 10838-128-3: DSCF3757.JPG
++++++ -/r * 10839-128-4: ScottSports.htm
++++++ -/r * 10840-128-4: Bornstein (an american chron TR).pdf
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
++++++ -/r * 10844-128-4: Classic_models_query.xps
++++++ -/r * 10845-128-3: DSCF3758.JPG
++++++ -/r * 10846-128-3: DSCF3719.JPG
++++++ -/r * 10847-128-4: Federal Reserve Locations.jpg
++++++ -/r * 10848-128-3: DSCF3690.JPG
+++++ r/- * 0: Reading_List.pdf
+++++ -/r * 10736-128-4: Bornstein (an american chron TR).pdf
+++++ -/r * 10849-128-3: Cookbook.pdf
+++ r/r 13950-128-4: Phone_track.pdf
+++ r/r 13950-128-5: Phone_track.pdf:Zone.Identifier
+++ r/r 13604-128-1: Please_read_this.txt
+++ r/r 10696-128-3: pscp.exe
+++ r/r 10696-128-4: pscp.exe:Zone.Identifier
+++ r/r 10690-128-3: putty.exe
Plain Text
Tab Width: 8
Ln 767, Col 62
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: sentations/Wednesday/Federal.jpg
Browse
iNode number: 10847-128-4
Extract files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:46


Find
Search for:
Federal Reserve
Match case
Match entire word only
Search backwards
Wrap around
Close
Computer
Home
Presentations
Cyber Discovery
Federal.jpg
Image Edit View Go Help
Previous
Next
HYDRAULIC CYLINDER
Hideki Hata, Yokohama (Japan)
Assigned to Hitachi Automotive Systems, Ltd., Ibaraki (Japan)
Filed by Hideki Hata, Yokohama (Japan)
Claims priority of application No. 2009-155224 (JP), filed on Jun. 30, 2009.
Prior Publication 010/0326267 A1, Dec. 30, 2010
U.S. Cl. 91 [188/266.6] 5 Claims
773 × 936 pixels 211.7 kB 59% 1 / 2
Wednesday
File Edit View Go Bookmarks Help
Wednesday
hdimage
Italia.jpg
listing.txt
Phone_track.pdf
Phone_track.pdf:Zone.Identifier
Please_read_this.txt
pscp.exe
pscp.exe:Zone.Identifier
putty.exe
Plain Text
Tab Width: 8
Ln 767, Col 62
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file:
Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
sentations/Wednesday/Federal.jpg
Browse
iNode number:
10847-128-4
Extract files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
Federal.jpg
19:47


Find
Search for: California
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: sentations/Wednesday/Federal.jpg
Browse
iNode number: 10847-128-4
Extract files
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
Federal.jpg
hdimage
Italia.jpg
listing.txt
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ -/r * 10819-128-3: en.htm
++++++ -/r * 10820-128-4: intelligence-literature.htm
++++++ -/r * 10821-128-3: DSCF3775.JPG
++++++ -/r * 10822-128-3: DSCF3727.JPG
++++++ -/r * 10823-128-3: DSCF3785.JPG
++++++ -/r * 10826-128-3: DSCF3784.JPG
++++++ -/r * 10827-128-3: DSCF3728.JPG
++++++ -/r * 10828-128-4: Brown (debate immigration TR).pdf
++++++ -/r * 10829-128-3: DSCF3772.JPG
++++++ -/r * 10830-128-3: DSCF3724.JPG
++++++ -/r * 10831-128-4: California.htm
++++++ -/r * 10832-128-3: DSCF3684.JPG
++++++ -/r * 10833-128-4: www.pandora.com.htm
++++++ -/r * 10834-128-3: DSCF3764.JPG
++++++ -/r * 10836-128-3: DSCF3781.JPG
++++++ -/r * 10837-128-4: www.menswearhouse.com.htm
++++++ -/r * 10838-128-3: DSCF3757.JPG
++++++ -/r * 10839-128-4: ScottSports.htm
++++++ -/r * 10840-128-4: Bornstein (an american chron TR).pdf
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
++++++ -/r * 10844-128-4: Classic_models_query.xps
Plain Text
Tab Width: 8
Ln 753, Col 47
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:47
PowerBook G4


Find
Search for: California
Match case
Match entire word only
Search backwards
Wrap around
Close
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
listing.txt
Result
MFT Entry Header Values:
Entry: 10831 Sequence: 4
$LogFile Sequence Number: 42571555
Not Allocated File
Links: 2
$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 359 (S-1-5-21-1177238915-1343024091-1435490099-1003)
Created: 2015-07-15 10:36:06 (CDT)
File Modified: 2015-07-15 10:36:06 (CDT)
MFT Modified: 2015-07-15 10:36:06 (CDT)
Accessed: 2015-07-15 10:36:06 (CDT)
$FILE_NAME Attribute Values:
Flags: Archive
Name: California.htm
Parent MFT Entry: 10737 Sequence: 3
Allocated Size: 0 Actual Size: 0
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10831-128-4
Working...
Wednesday) - gedit
++++++ -/r * 10838-128-3: DSCF3757.JPG
++++++ -/r * 10839-128-4: ScottSports.htm
++++++ -/r * 10840-128-4: Bornstein (an american chron TR).pdf
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
Plain Text
Tab Width: 8
Ln 753, Col 47
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:48


Find
Search for: California
Match case
Match entire word only
Search backwards
Wrap around
Close
Wednesday
File Edit View Go Bookmarks Help
cyber Desktop Presentations Wednesday
My Computer
Home
Desktop
listing.txt
Result
$FILE_NAME Attribute Values:
Flags: Archive
Name: California.htm
Parent MFT Entry: 10737 Sequence: 3
Allocated Size: 0 Actual Size: 0
Created: 2015-07-15 10:36:06 (CDT)
File Modified: 2015-07-15 10:36:06 (CDT)
MFT Modified: 2015-07-15 10:36:06 (CDT)
Accessed: 2015-07-15 10:36:06 (CDT)
Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 90
Type: $FILE_NAME (48-2) Name: N/A Resident size: 94
Type: $DATA (128-4) Name: N/A Non-Resident size: 121592 init_size: 121592
1132604 1132605 1132606 1132607 1132608 1132609 1132610 1132611
1132612 1132613 1132614 1132615 1132616 1132617 1132618 1132619
1132620 1132621 1131781 1131782 1131783 1131784 1131785 1131786
1185682 1185683 1185684 1185685 1185686 1185687
OK
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file:
Browse
iNode number: 10831-128-4
Working...
Wednesday) - gedit
++++++ -/r * 10838-128-3: DSCF3757.JPG
++++++ -/r * 10839-128-4: ScottSports.htm
++++++ -/r * 10840-128-4: Bornstein (an american chron TR).pdf
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
Plain Text
Tab Width: 8
Ln 753, Col 47
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:48
Computer
Home
Presentations
Cyber Discovery


Find
Search for: California
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: ntations/Wednesday/California.htm
Browse
iNode number: 10831-128-4
Extract files
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
California.htm
Federal.jpg
hdimage
Italia.jpg
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ -/r * 10819-128-3: en.htm
++++++ -/r * 10820-128-4: intelligence-literature.htm
++++++ -/r * 10821-128-3: DSCF3775.JPG
++++++ -/r * 10822-128-3: DSCF3727.JPG
++++++ -/r * 10823-128-3: DSCF3785.JPG
++++++ -/r * 10826-128-3: DSCF3784.JPG
++++++ -/r * 10827-128-3: DSCF3728.JPG
++++++ -/r * 10828-128-4: Brown (debate immigration TR).pdf
++++++ -/r * 10829-128-3: DSCF3772.JPG
++++++ -/r * 10830-128-3: DSCF3724.JPG
++++++ -/r * 10831-128-4: California.htm
++++++ -/r * 10832-128-3: DSCF3684.JPG
++++++ -/r * 10833-128-4: www.pandora.com.htm
++++++ -/r * 10834-128-3: DSCF3764.JPG
++++++ -/r * 10836-128-3: DSCF3781.JPG
++++++ -/r * 10837-128-4: www.menswearhouse.com.htm
++++++ -/r * 10838-128-3: DSCF3757.JPG
++++++ -/r * 10839-128-4: ScottSports.htm
++++++ -/r * 10840-128-4: Bornstein (an american chron TR).pdf
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
++++++ -/r * 10844-128-4: Classic_models_query.xps
Plain Text
Tab Width: 8
Ln 753, Col 47
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:49


Find
Search for: California
Match case
Wednesday
File Edit View Go Bookmarks Help
cyber Desktop Presentations Wednesday
Computer
Home
Presentations
Cyber Discovery
Italia.jpg
California - Surfing in California, United States of America - WannaSurf, surf spots atlas, surfing photos, maps, GPS location - Mozilla Firefox
California - Surfing in Californ...
file:///home/cyber/Desktop/Presentations/Wednesday/California.htm
Search
Most Visited Linux Mint Community Forums Blog News
Home
Store
Professionals
Help
English
Español
Français
Português
Other language?
Community
Login
Username
Login
Lost password? New user? Register
My Surf
My Profile
Program Forensics
Select image file:
Save re
Select output file:
iNode number: 10831-128-4
Extract files
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
Plain Text Tab Width: 8 Ln 753, Col 47 INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
California - Surfing i...
19:49


Find
Search for: California
Match case
Wednesday
File Edit View Go Bookmarks Help
cyber Desktop Presentations Wednesday
Computer
Home
Presentations
Cyber Discovery
California - Surfing in California, United States of America - WannaSurf, surf spots atlas, surfing photos, maps, GPS location - Mozilla Firefox
California - Surfing in Californ...
file:///home/cyber/Desktop/Presentations/Wednesday/California.htm
Search
Most Visited Linux Mint Community Forums Blog News
NEVADA
CALIFORNIA
Google
Map data ©2015 Google, INEGI Imagery ©2015 TerraMetrics
Tweet 0
Like 36
Italia.jpg
Program Forensics
Select image file:
Save re
Select output file:
iNode number: 10831-128-4
Extract files
++++++ -/r * 10841-128-3: DSCF3717.JPG
++++++ -/r * 10842-128-3: DSCF3782.JPG
Plain Text Tab Width: 8 Ln 753, Col 47 INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
California - Surfing i...
19:49

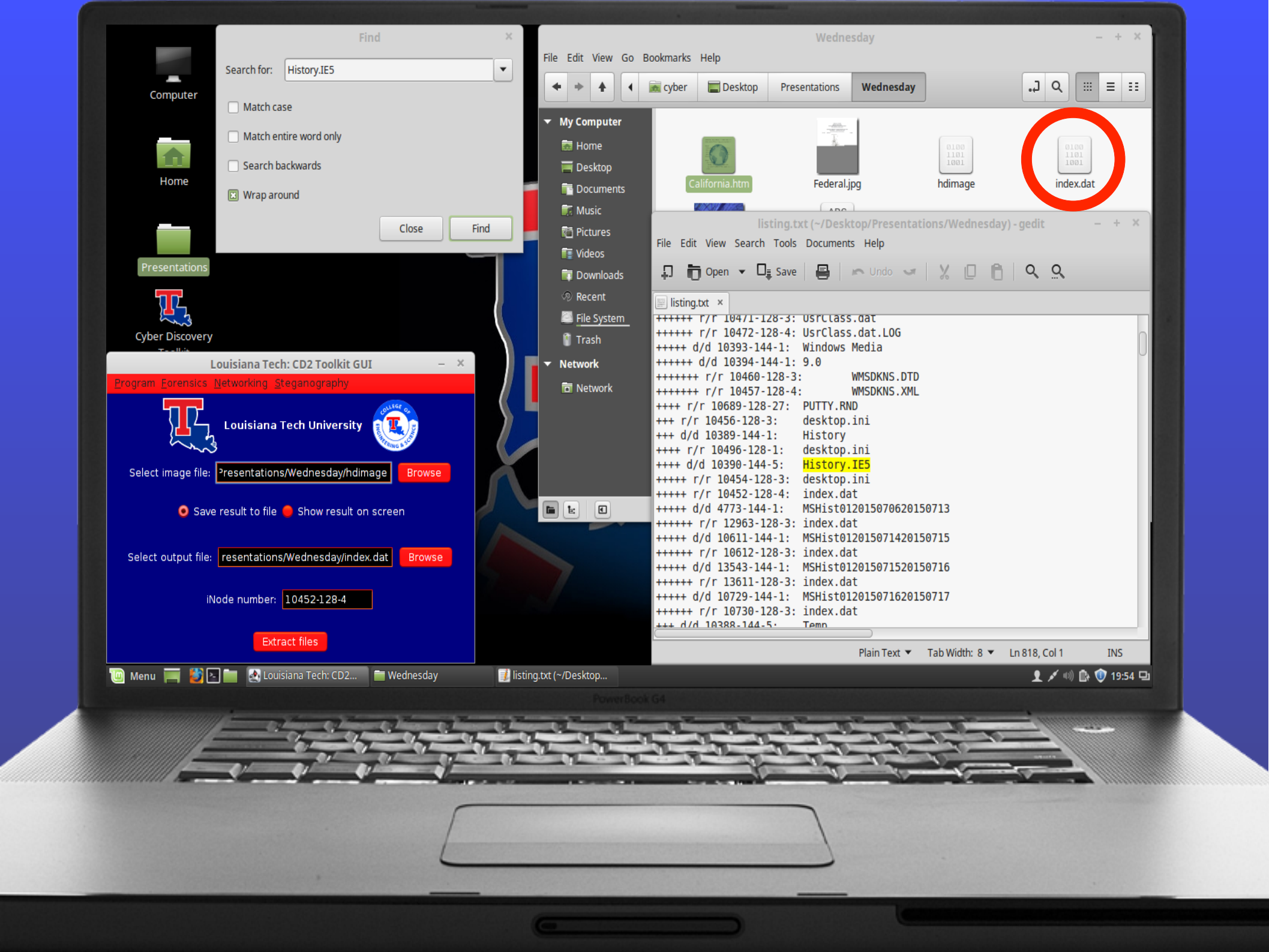
Browser History

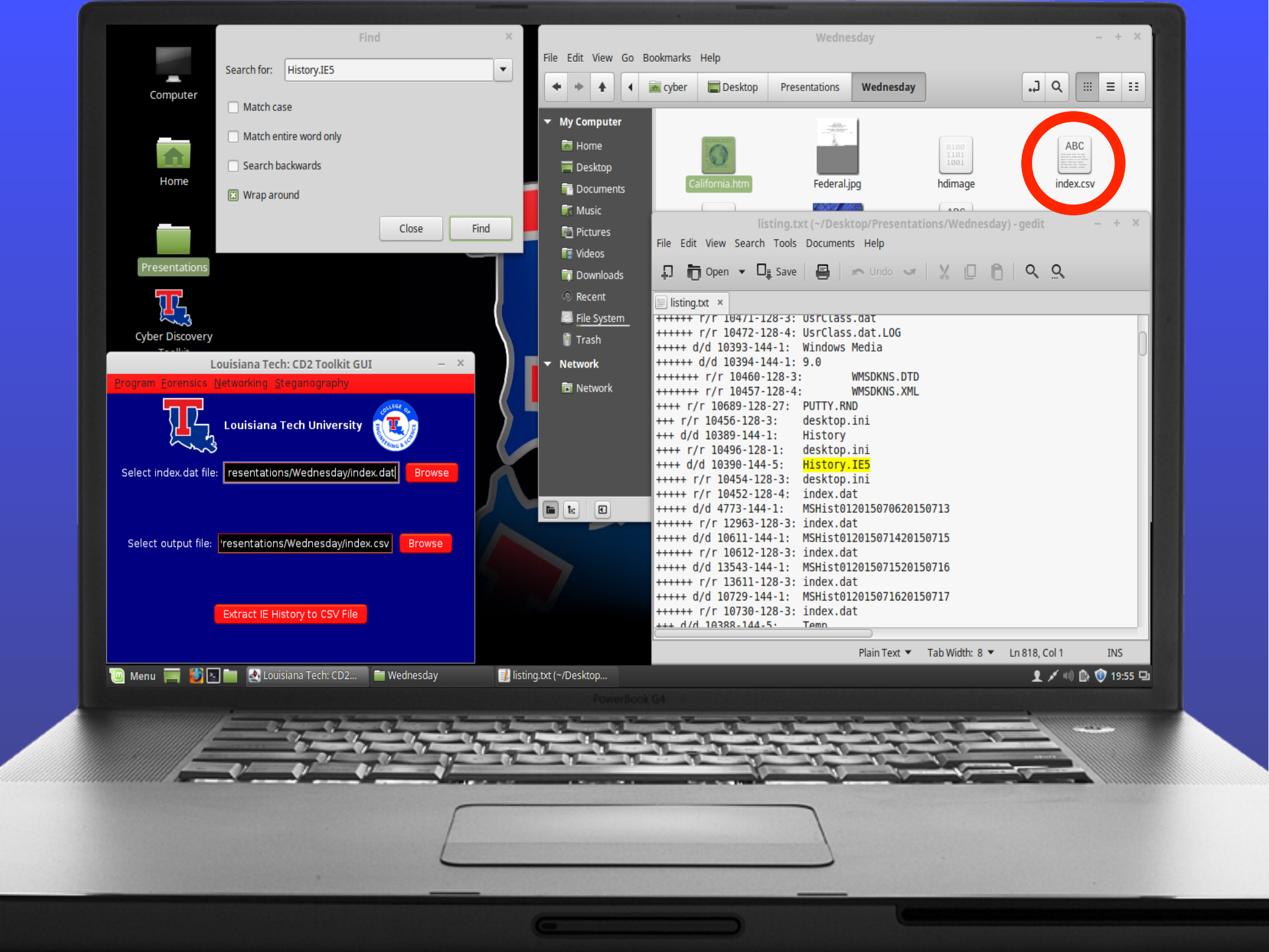
- Let's look at Web Browser History
- Where is the browser history stored?
  - Internet Explorer – `index.dat`
  - Firefox – `history.dat` (older versions) or `places.sqlite` (version 3 and above)
  - Chrome – `history.sqlite`
- Internet Explorer
  - Lots of `index.dat` files
  - Search for **History.IE5**
  - Also, can look for the ones associated with a `MSHist`*`date`* directory
  - Example:

```
+++++ d/d 4773-144-1: MSHist012015070620150713
++++++ r/r 12693-128-3: index.dat
```

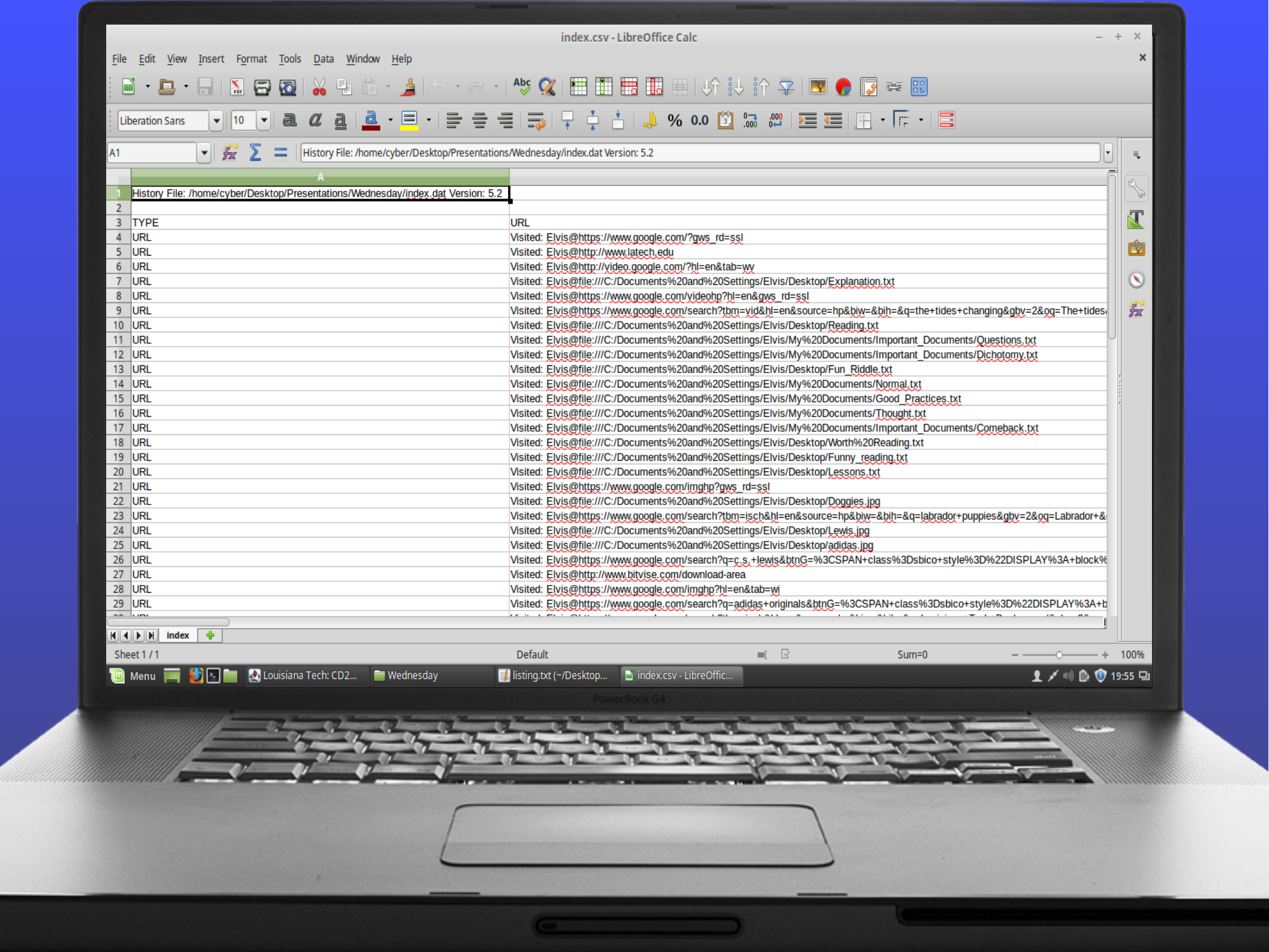
CYBER DISCOVERY

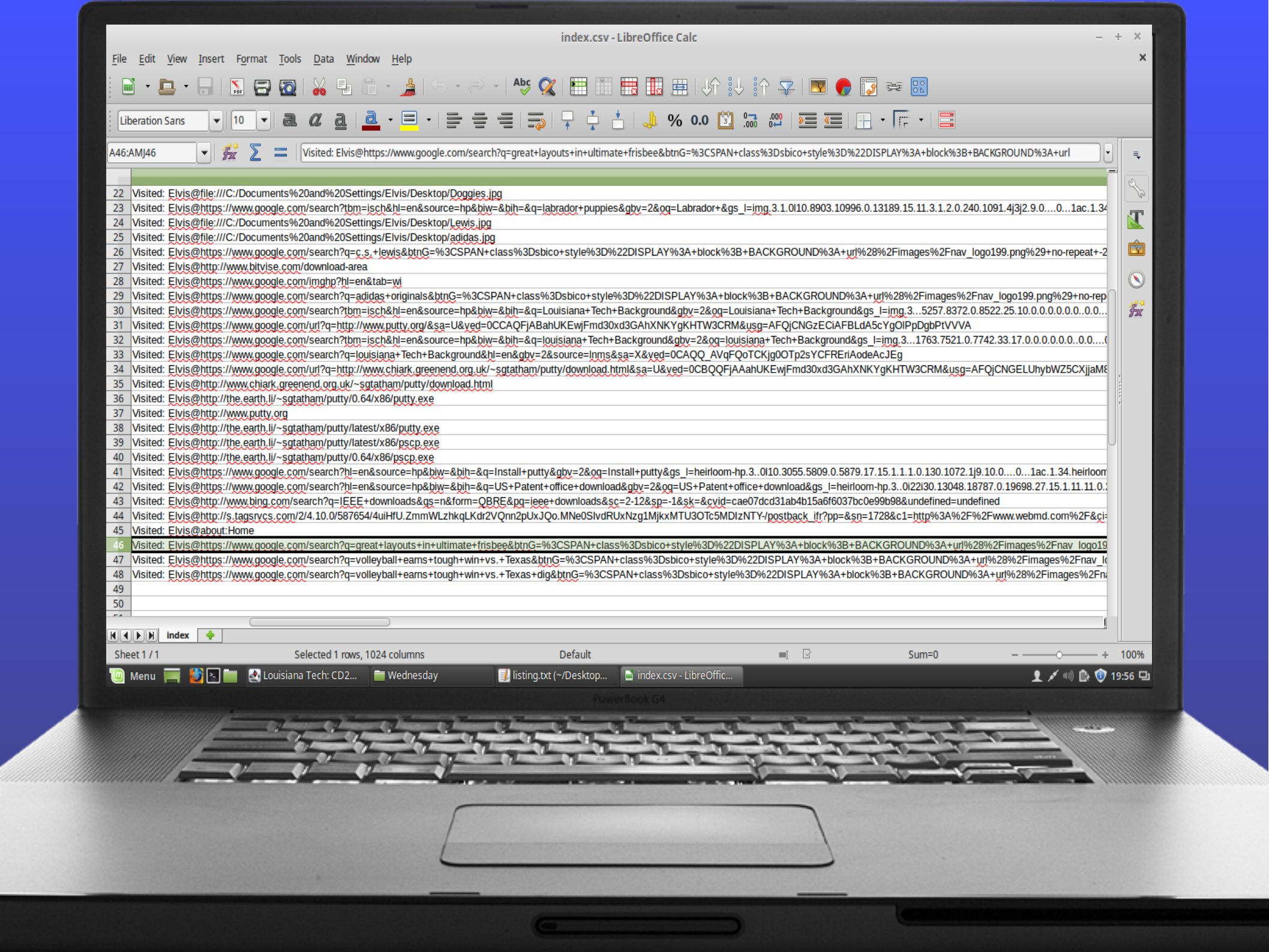

Find
Search for: History.IE5
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
California.htm
Federal.jpg
hdimage
Italia.jpg
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ r/r 10471-128-3: UsrClass.dat
++++++ r/r 10472-128-4: UsrClass.dat.LOG
+++++ d/d 10393-144-1: Windows Media
++++++ d/d 10394-144-1: 9.0
+++++++ r/r 10460-128-3: WMSDKNS.DTD
+++++++ r/r 10457-128-4: WMSDKNS.XML
++++ r/r 10689-128-27: PUTTY.RND
+++ r/r 10456-128-3: desktop.ini
+++ d/d 10389-144-1: History
++++ r/r 10496-128-1: desktop.ini
++++ d/d 10390-144-5: History.IE5
+++++ r/r 10454-128-3: desktop.ini
+++++ r/r 10452-128-4: index.dat
+++++ d/d 4773-144-1: MSHist012015070620150713
++++++ r/r 12963-128-3: index.dat
+++++ d/d 10611-144-1: MSHist012015071420150715
++++++ r/r 10612-128-3: index.dat
+++++ d/d 13543-144-1: MSHist012015071520150716
++++++ r/r 13611-128-3: index.dat
+++++ d/d 10729-144-1: MSHist012015071620150717
++++++ r/r 10730-128-3: index.dat
+++ d/d 10388-144-5: Temp
Plain Text
Tab Width: 8
Ln 818, Col 1
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: ntations/Wednesday/California.htm
Browse
iNode number: 10831-128-4
Extract files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:53

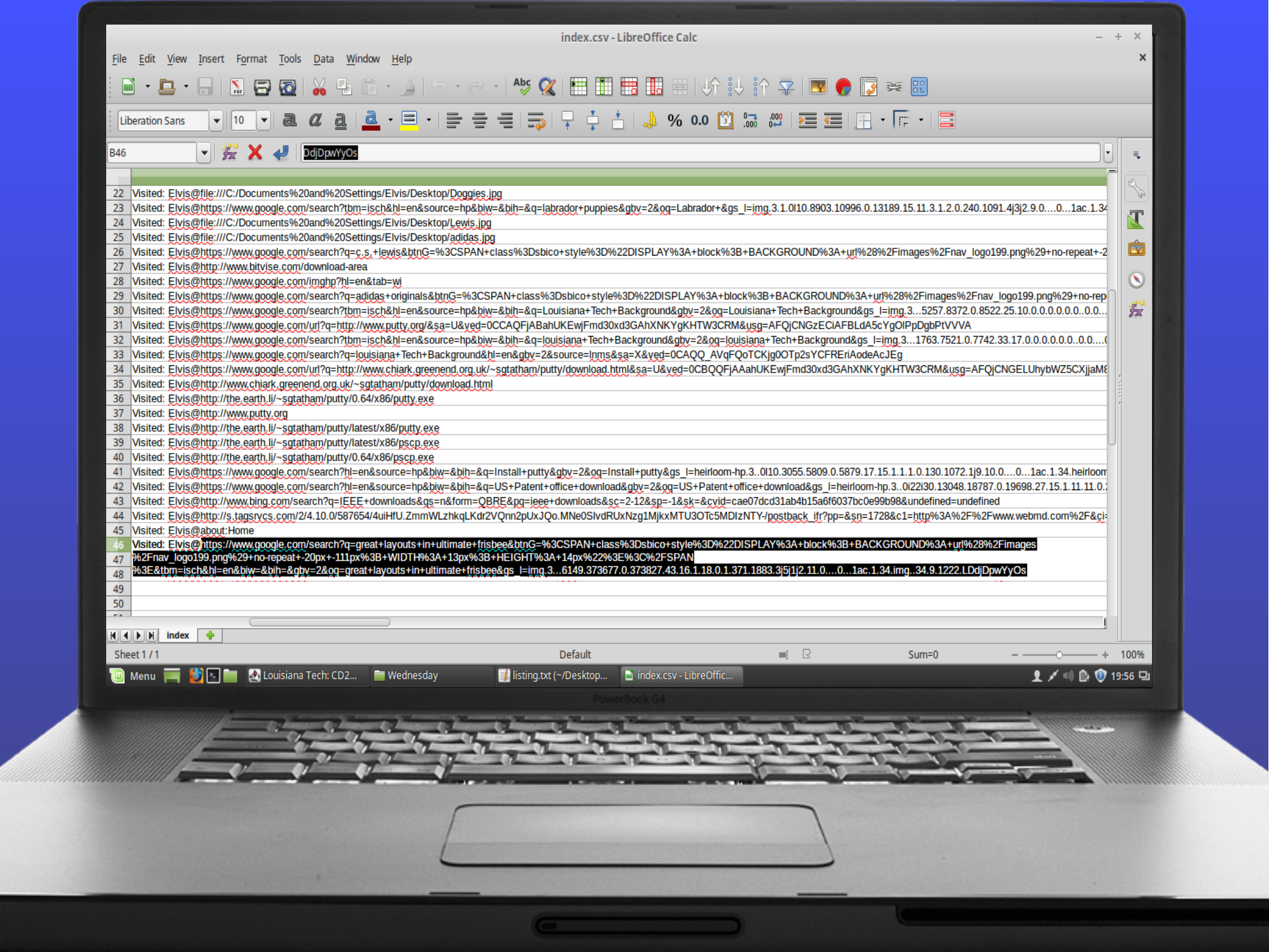

Find
Search for: History.IE5
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
California.htm
Federal.jpg
hdimage
index.dat
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ r/r 10471-128-3: UsrClass.dat
++++++ r/r 10472-128-4: UsrClass.dat.LOG
+++++ d/d 10393-144-1: Windows Media
++++++ d/d 10394-144-1: 9.0
+++++++ r/r 10460-128-3: WMSDKNS.DTD
+++++++ r/r 10457-128-4: WMSDKNS.XML
++++ r/r 10689-128-27: PUTTY.RND
+++ r/r 10456-128-3: desktop.ini
+++ d/d 10389-144-1: History
++++ r/r 10496-128-1: desktop.ini
++++ d/d 10390-144-5: History.IE5
+++++ r/r 10454-128-3: desktop.ini
+++++ r/r 10452-128-4: index.dat
+++++ d/d 4773-144-1: MSHist012015070620150713
++++++ r/r 12963-128-3: index.dat
+++++ d/d 10611-144-1: MSHist012015071420150715
++++++ r/r 10612-128-3: index.dat
+++++ d/d 13543-144-1: MSHist012015071520150716
++++++ r/r 13611-128-3: index.dat
+++++ d/d 10729-144-1: MSHist012015071620150717
++++++ r/r 10730-128-3: index.dat
Plain Text
Tab Width: 8
Ln 818, Col 1
INS
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select image file: Presentations/Wednesday/hdimage
Browse
Save result to file
Show result on screen
Select output file: resentations/Wednesday/index.dat
Browse
iNode number: 10452-128-4
Extract files
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:54

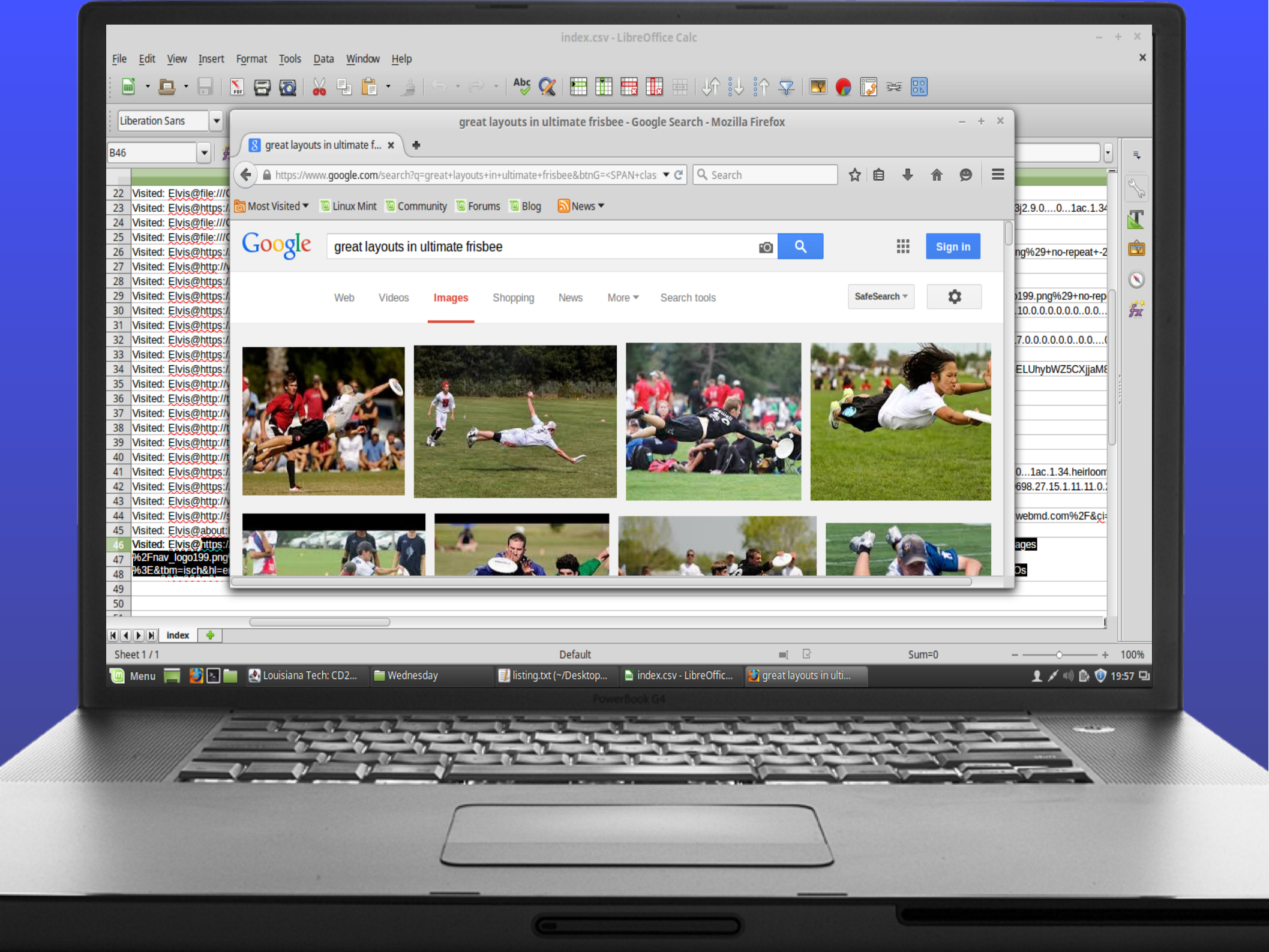

Find
Search for: History.IE5
Match case
Match entire word only
Search backwards
Wrap around
Close
Find
Computer
Home
Presentations
Cyber Discovery
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select index.dat file: resentations/Wednesday/index.dat
Browse
Select output file: 'resentations/Wednesday/index.csv
Browse
Extract IE History to CSV File
Wednesday
File Edit View Go Bookmarks Help
cyber
Desktop
Presentations
Wednesday
My Computer
Home
Desktop
Documents
Music
Pictures
Videos
Downloads
Recent
File System
Trash
Network
Network
California.htm
Federal.jpg
hdimage
index.csv
listing.txt (~/Desktop/Presentations/Wednesday) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
listing.txt
++++++ r/r 10471-128-3: UsrClass.dat
++++++ r/r 10472-128-4: UsrClass.dat.LOG
+++++ d/d 10393-144-1: Windows Media
++++++ d/d 10394-144-1: 9.0
+++++++ r/r 10460-128-3: WMSDKNS.DTD
+++++++ r/r 10457-128-4: WMSDKNS.XML
++++ r/r 10689-128-27: PUTTY.RND
+++ r/r 10456-128-3: desktop.ini
+++ d/d 10389-144-1: History
++++ r/r 10496-128-1: desktop.ini
++++ d/d 10390-144-5: History.IE5
+++++ r/r 10454-128-3: desktop.ini
+++++ r/r 10452-128-4: index.dat
+++++ d/d 4773-144-1: MSHist012015070620150713
++++++ r/r 12963-128-3: index.dat
+++++ d/d 10611-144-1: MSHist012015071420150715
++++++ r/r 10612-128-3: index.dat
+++++ d/d 13543-144-1: MSHist012015071520150716
++++++ r/r 13611-128-3: index.dat
+++++ d/d 10729-144-1: MSHist012015071620150717
++++++ r/r 10730-128-3: index.dat
+++ d/d 10388-144-5: Temp
Plain Text
Tab Width: 8
Ln 818, Col 1
INS
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
19:55


Find
Search for: History.IE5
Match case
Match entire word only
Search backwards
Wrap around
Computer
Home
Presentations
Cyber Discovery
Wednesday
File Edit View Go Bookmarks Help
Wednesday
hdimage
index.csv
listing.txt
Free space: 268.3 GB
015071420150715
015071520150716
015071620150717
Plain Text
Tab Width: 8
Ln 818, Col 1
INS
Text Import - [index.csv]
Import
Character set:
Language: Default - English (USA)
From row: 1
Separator Options
Fixed width
Separated by
Tab
Comma
Semicolon
Space
Other
Merge delimiters
Text delimiter: "
Other Options
Quoted field as text
Detect special numbers
Fields
Column type:
Standard
1 History File: /home/cyber/Desktop/Presentations/Wednesday/index.dat Version
2
3 TYPE
4 URL
5 URL
6 URL
7 URL
8 URL
9 URL
Help
OK
Cancel
Louisiana Tech: CD2 Toolkit GUI
Program Forensics Networking Steganography
Louisiana Tech University
Select index.dat file: resentations/Wednesday/index.dat
Select output file: 'resentations/Wednesday/index.csv
Extract IE History to CSV File
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
Text Import - [index....
19:55


index.csv - LibreOffice Calc
File Edit View Insert Format Tools Data Window Help
Liberation Sans 10
A1
History File: /home/cyber/Desktop/Presentations/Wednesday/index.dat Version: 5.2
A
1 History File: /home/cyber/Desktop/Presentations/Wednesday/index.dat Version: 5.2
2
3 TYPE URL
4 URL Visited: Elvis@https://www.google.com/?gws_rd=ssl
5 URL Visited: Elvis@http://www.latech.edu
6 URL Visited: Elvis@http://video.google.com/?hl=en&tab=wv
7 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Explanation.txt
8 URL Visited: Elvis@https://www.google.com/videohp?hl=en&gws_rd=ssl
9 URL Visited: Elvis@https://www.google.com/search?tbm=vid&hl=en&source=hp&biw=&bih=&q=the+tides+changing&gbv=2&oq=The+tides
10 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Reading.txt
11 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/My%20Documents/Important_Documents/Questions.txt
12 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/My%20Documents/Important_Documents/Dichotomy.txt
13 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Fun_Riddle.txt
14 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/My%20Documents/Normal.txt
15 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/My%20Documents/Good_Practices.txt
16 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/My%20Documents/Thought.txt
17 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/My%20Documents/Important_Documents/Comeback.txt
18 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Worth%20Reading.txt
19 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Funny_reading.txt
20 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Lessons.txt
21 URL Visited: Elvis@https://www.google.com/imghp?gws_rd=ssl
22 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Doggies.jpg
23 URL Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=labrador+puppies&gbv=2&oq=Labrador+&
24 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Lewis.jpg
25 URL Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/adidas.jpg
26 URL Visited: Elvis@https://www.google.com/search?q=c.s.+lewis&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%
27 URL Visited: Elvis@http://www.bitvise.com/download-area
28 URL Visited: Elvis@https://www.google.com/imghp?hl=en&tab=wi
29 URL Visited: Elvis@https://www.google.com/search?q=adidas+originals&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+b
index
Sheet 1 / 1
Default
Sum=0
100%
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
index.csv - LibreOffic...
19:55


index.csv - LibreOffice Calc
File Edit View Insert Format Tools Data Window Help
Liberation Sans 10
A46:AMJ46
Visited: Elvis@https://www.google.com/search?q=great+layouts+in+ultimate+frisbee&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url
22 Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Doggies.jpg
23 Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=labrador+puppies&gbv=2&oq=Labrador+&gs_l=img.3.1.0l10.8903.10996.0.13189.15.11.3.1.2.0.240.1091.4j3j2.9.0....0...1ac.1.34
24 Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Lewis.jpg
25 Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/adidas.jpg
26 Visited: Elvis@https://www.google.com/search?q=c.s.+lewis&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fnav_logo199.png%29+no-repeat+-2
27 Visited: Elvis@http://www.bitvise.com/download-area
28 Visited: Elvis@https://www.google.com/imghp?hl=en&tab=wi
29 Visited: Elvis@https://www.google.com/search?q=adidas+originals&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fnav_logo199.png%29+no-rep
30 Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=Louisiana+Tech+Background&gbv=2&oq=Louisiana+Tech+Background&gs_l=img.3...5257.8372.0.8522.25.10.0.0.0.0.0.0..0.0...
31 Visited: Elvis@https://www.google.com/url?q=http://www.putty.org/&sa=U&ved=0CCAQFjABahUKEwjFmd30xd3GAhXNKYgKHTW3CRM&usg=AFQjCNGzECiAFBLdA5cYgOlPpDgbPtVVVA
32 Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=louisiana+Tech+Background&gbv=2&oq=louisiana+Tech+Background&gs_l=img.3...1763.7521.0.7742.33.17.0.0.0.0.0.0..0.0....(
33 Visited: Elvis@https://www.google.com/search?q=louisiana+Tech+Background&hl=en&gbv=2&source=lnms&sa=X&ved=0CAQQ_AVqFQoTCKjg0OTp2sYCFRERiAodeAcJEg
34 Visited: Elvis@https://www.google.com/url?q=http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html&sa=U&ved=0CBQQFjAAahUKEwjFmd30xd3GAhXNKYgKHTW3CRM&usg=AFQjCNGELUhybWZ5CXjjaM8
35 Visited: Elvis@http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
36 Visited: Elvis@http://the.earth.li/~sgtatham/putty/0.64/x86/putty.exe
37 Visited: Elvis@http://www.putty.org
38 Visited: Elvis@http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
39 Visited: Elvis@http://the.earth.li/~sgtatham/putty/latest/x86/pscp.exe
40 Visited: Elvis@http://the.earth.li/~sgtatham/putty/0.64/x86/pscp.exe
41 Visited: Elvis@https://www.google.com/search?hl=en&source=hp&biw=&bih=&q=Install+putty&gbv=2&oq=Install+putty&gs_l=heirloom-hp.3..0l10.3055.5809.0.5879.17.15.1.1.1.0.130.1072.1j9.10.0....0...1ac.1.34.heirloom
42 Visited: Elvis@https://www.google.com/search?hl=en&source=hp&biw=&bih=&q=US+Patent+office+download&gbv=2&oq=US+Patent+office+download&gs_l=heirloom-hp.3..0i22i30.13048.18787.0.19698.27.15.1.11.11.0.
43 Visited: Elvis@http://www.bing.com/search?q=IEEE+downloads&qs=n&form=QBRE&pq=ieee+downloads&sc=2-12&sp=-1&sk=&cvid=cae07dcd31ab4b15a6f6037bc0e99b98&undefined=undefined
44 Visited: Elvis@http://s.tagsrvcs.com/2/4.10.0/587654/4uiHfU.ZmmWLzhkqLKdr2VQnn2pUxJQo.MNe0SlvdRUxNzg1MjkxMTU3OTc5MDIzNTY-/postback_ifr?pp=&sn=1728&c1=http%3A%2F%2Fwww.webmd.com%2F&ci=
45 Visited: Elvis@about:Home
46 Visited: Elvis@https://www.google.com/search?q=great+layouts+in+ultimate+frisbee&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fnav_logo19
47 Visited: Elvis@https://www.google.com/search?q=volleyball+earns+tough+win+vs.+Texas&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fnav_l
48 Visited: Elvis@https://www.google.com/search?q=volleyball+earns+tough+win+vs.+Texas+dig&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fna
49
50
index
Sheet 1 / 1
Selected 1 rows, 1024 columns
Default
Sum=0
100%
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
index.csv - LibreOffic...
19:56
PowerBook G4


index.csv - LibreOffice Calc
File Edit View Insert Format Tools Data Window Help
Liberation Sans 10
B46
0djDpwYyOs
22 Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Doggies.jpg
23 Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=labrador+puppies&gbv=2&oq=Labrador+&gs_l=img.3.1.0l10.8903.10996.0.13189.15.11.3.1.2.0.240.1091.4j3j2.9.0....0...1ac.1.34
24 Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/Lewis.jpg
25 Visited: Elvis@file:///C:/Documents%20and%20Settings/Elvis/Desktop/adidas.jpg
26 Visited: Elvis@https://www.google.com/search?q=c.s.+lewis&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fnav_logo199.png%29+no-repeat+-2
27 Visited: Elvis@http://www.bitvise.com/download-area
28 Visited: Elvis@https://www.google.com/imghp?hl=en&tab=wi
29 Visited: Elvis@https://www.google.com/search?q=adidas+originals&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages%2Fnav_logo199.png%29+no-rep
30 Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=Louisiana+Tech+Background&gbv=2&oq=Louisiana+Tech+Background&gs_l=img.3...5257.8372.0.8522.25.10.0.0.0.0.0.0..0.0...
31 Visited: Elvis@https://www.google.com/url?q=http://www.putty.org/&sa=U&ved=0CCAQFjABahUKEwjFmd30xd3GAhXNKYgKHTW3CRM&usg=AFQjCNGzECiAFBLdA5cYgOlPpDgbPtVVVA
32 Visited: Elvis@https://www.google.com/search?tbm=isch&hl=en&source=hp&biw=&bih=&q=louisiana+Tech+Background&gbv=2&oq=louisiana+Tech+Background&gs_l=img.3...1763.7521.0.7742.33.17.0.0.0.0.0.0..0.0....(
33 Visited: Elvis@https://www.google.com/search?q=louisiana+Tech+Background&hl=en&gbv=2&source=lnms&sa=X&ved=0CAQQ_AVqFQoTCKjg0OTp2sYCFRERiAodeAcJEg
34 Visited: Elvis@https://www.google.com/url?q=http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html&sa=U&ved=0CBQQFjAAahUKEwjFmd30xd3GAhXNKYgKHTW3CRM&usg=AFQjCNGELUhybWZ5CXjjaM8
35 Visited: Elvis@http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
36 Visited: Elvis@http://the.earth.li/~sgtatham/putty/0.64/x86/putty.exe
37 Visited: Elvis@http://www.putty.org
38 Visited: Elvis@http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
39 Visited: Elvis@http://the.earth.li/~sgtatham/putty/latest/x86/pscp.exe
40 Visited: Elvis@http://the.earth.li/~sgtatham/putty/0.64/x86/pscp.exe
41 Visited: Elvis@https://www.google.com/search?hl=en&source=hp&biw=&bih=&q=Install+putty&gbv=2&oq=Install+putty&gs_l=heirloom-hp.3..0l10.3055.5809.0.5879.17.15.1.1.1.0.130.1072.1j9.10.0....0...1ac.1.34.heirloom
42 Visited: Elvis@https://www.google.com/search?hl=en&source=hp&biw=&bih=&q=US+Patent+office+download&gbv=2&oq=US+Patent+office+download&gs_l=heirloom-hp.3..0i22i30.13048.18787.0.19698.27.15.1.11.11.0.
43 Visited: Elvis@http://www.bing.com/search?q=IEEE+downloads&qs=n&form=QBRE&pq=ieee+downloads&sc=2-12&sp=-1&sk=&cvid=cae07dcd31ab4b15a6f6037bc0e99b98&undefined=undefined
44 Visited: Elvis@http://s.tagsrvcs.com/2/4.10.0/587654/4uiHfU.ZmmWLzhkqLKdr2VQnn2pUxJQo.MNe0SlvdRUxNzg1MjkxMTU3OTc5MDIzNTY-/postback_ifr?pp=&sn=1728&c1=http%3A%2F%2Fwww.webmd.com%2F&ci=
45 Visited: Elvis@about:Home
46 Visited: Elvis@https://www.google.com/search?q=great+layouts+in+ultimate+frisbee&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+BACKGROUND%3A+url%28%2Fimages
47 %2Fnav_logo199.png%29+no-repeat+-20px+-111px%3B+WIDTH%3A+13px%3B+HEIGHT%3A+14px%22%3E%3C%2FSPAN
48 %3E&tbm=isch&hl=en&biw=&bih=&gbv=2&oq=great+layouts+in+ultimate+frisbee&gs_l=img.3...6149.373677.0.373827.43.16.1.18.0.1.371.1883.3j5j1j2.11.0....0...1ac.1.34.img..34.9.1222.LDdjDpwYyOs
49
50
index
Sheet 1 / 1
Default
Sum=0
100%
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
index.csv - LibreOffic...
19:56
PowerBook G4


index.csv - LibreOffice Calc
File Edit View Insert Format Tools Data Window Help
great layouts in ultimate frisbee - Google Search - Mozilla Firefox
great layouts in ultimate f...
https://www.google.com/search?q=great+layouts+in+ultimate+frisbee&btnG=<SPAN+clas
Search
Most Visited Linux Mint Community Forums Blog News
Google
great layouts in ultimate frisbee
Sign in
Web Videos Images Shopping News More Search tools
SafeSearch
Visited: Elvis@file:///C
Visited: Elvis@https:/
Visited: Elvis@file:///C
Visited: Elvis@file:///C
Visited: Elvis@https:/
Visited: Elvis@http://v
Visited: Elvis@https:/
Visited: Elvis@https:/
Visited: Elvis@https:/
Visited: Elvis@https:/
Visited: Elvis@https:/
Visited: Elvis@http://v
Visited: Elvis@http://t
Visited: Elvis@http://v
Visited: Elvis@http://t
Visited: Elvis@http://t
Visited: Elvis@http://t
Visited: Elvis@https:/
Visited: Elvis@https:/
Visited: Elvis@http://v
Visited: Elvis@http://s
Visited: Elvis@about:
Visited: Elvis@https:/
%2Fnav_logo199.png
%3E&tbm=isch&hl=e
index
Sheet 1 / 1
Default
Sum=0
100%
Menu
Louisiana Tech: CD2...
Wednesday
listing.txt (~/Desktop...
index.csv - LibreOffic...
great layouts in ulti...
19:57

Hard Drive Analysis

- Now it's your turn
  - See if you can find the following files and see if you can extract the
  - Or you can begin your own investigation of the sample disk image and see what you can find

```
Instructions.txt
Fun_Riddle.txt
maserati.jpg
VBDig.jpg
ET.wav
```

CYBER DISCOVERY

Investigating a Crime Scene

- Investigating a scene
  - Be very observant of the surroundings
  - Listen to see is the computer is on
    - If the monitor is on, note what is on the screen
    - Look for indications of suspect trying to cover up activities
    - Look for a web cam and see if active
    - Look for evidence of ongoing communication
      - Look for wireless access points
  - Look around and identify all digital devices

CYBER DISCOVERY

Investigating a Crime Scene

- Investigating a scene
  - Take pictures of how everything is set ip
  - Look at papers on desk
    - Is there anything there that may provide any clues?
      - Passwords written on Post-It notes
        - These could be under the keyboard or on the monitor
      - Notepads with information written on them
  - Document everything before anything is touched
  - Roam around the room look at everything from multiple angles
    - You never what may be hidden on first glance

CYBER DISCOVERY

Basic Cryptography

- Cryptography
  - Enciphering and deciphering of messages in secret code
- Cryptanalysis
  - Solving of cryptography systems (to decrypt secret messages)
- Cryptology
  - Study of cryptography and cryptanalysis

CYBER DISCOVERY

Basic Cryptography

- Many different variants of cryptographic systems
- Focus on symmetric-key systems
  - Both parties, sender and receiver, share private key ("password")
  - Substitution ciphers
  - Caesar ciphers
  - Vigenère ciphers

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - V

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQ

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

CYBER DISCOVERY

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQK

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

CYBER DISCOVERY

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQKF

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

CYBER DISCOVERY

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQKFO

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQKFOF

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQKFOFU

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

CYBER DISCOVERY

Simple Substitution

- Plaintext/Ciphertext alphabet
- Plaintext
  - WARNING
- Ciphertext
  - VQKFOFU

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

Cryptanalysis

- Ciphertext but no alphabet

EDHUP

?

Cryptanalysis

- Ciphertext but no alphabet

"DXLFC NTF, BF NTVKUNTVBES

DXL QXF'V LFQUPSVTFQ VKBFCS. DXL

RLSV CUV LSUQ VX VKUN."

-RXKF AXF FULNTFF

CYBER DISCOVERY

Cryptanalysis

- Ciphertext but no alphabet

"DXLFC NTF, BF NTVKUNTVBES
DXL QXF'V LFQUPSVTFQ VKBFCS. DXL
RLSV CUV LSUQ VX VKUN."
-RXKF AXF FULNTFF

- Many strategies to solve cryptograms
  - Language specific
  - Frequency count
  - Contextual clues

CYBER DISCOVERY

Cryptanalysis

- Ciphertext but no alphabet

"DXLFC NTF, BF NTVKUNTVBES
DXL QXF'V LFQUPSVTFQ VKBFCS. DXL
RLSV CUV LSUQ VX VKUN."
-RXKF AXF FULNTFF

- Many strategies to solve cryptograms
  - Language specific
  - Frequency count
  - Contextual clues

CYBER DISCOVERY

Cryptanalysis

- Ciphertext but no alphabet

"DXLFC NTF, BF NTVKUNTVBES
DXL QXF'V LFQUPSVTFQ VKBFCS. DXL
RLSV CUV LSUQ VX VKUN."
-RXKF AXF FULNTFF

- Many strategies to solve cryptograms
  - Language specific
  - Frequency count
  - Contextual clues

CYBER DISCOVERY

Caesar Cipher

- Simple substitution using a shift of alphabet (wrapped around)

ROT13

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Caesar Cipher

A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22

- Can also look at the approach as modular arithmetic
  - Shift by 13 (ROT13)
  - What is 0 + 13?

Caesar Cipher

A	0	13	
B	1		
C	2		
D	3		
E	4		
F	5		
G	6		
H	7		
I	8		
J	9		
K	10		
L	11		
M	12		
N	13		
O	14		
P	15		
Q	16		
R	17		
S	18		
T	19		
U	20		
V	21		
W	22		

- What letter is 13?

Caesar Cipher

A	0	13	N
B	1		
C	2		
D	3		
E	4		
F	5		
G	6		
H	7		
I	8		
J	9		
K	10		
L	11		
M	12		
N	13		
O	14		
P	15		
Q	16		
R	17		
S	18		
T	19		
U	20		
V	21		
W	22		

- Can repeat for all values…

Caesar Cipher

A	0	13	N
B	1	14	O
C	2	15	P
D	3	16	Q
E	4	17	R
F	5	18	S
G	6	19	T
H	7	20	U
I	8	21	V
J	9	22	W
K	10	23	X
L	11	24	Y
M	12	25	Z
N	13	26	?
O	14	27	?
P	15	28	?
Q	16	29	?
R	17	20	?
S	18	31	?
T	19	32	?
U	20	33	?
V	21	34	?
W	22	35	?

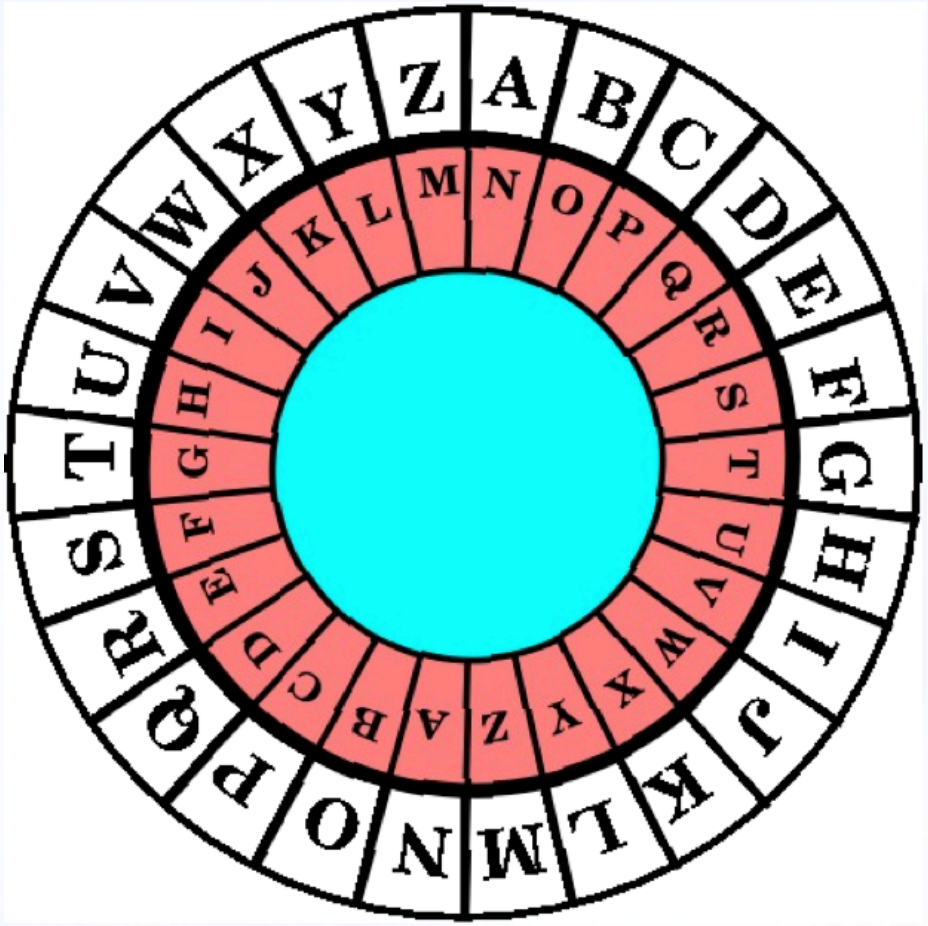
- But wait!
  - What is 13+13
  - Z is 25
  - So, what letter is 26?

Caesar Cipher

A	0	13	N
B	1	14	O
C	2	15	P
D	3	16	Q
E	4	17	R
F	5	18	S
G	6	19	T
H	7	20	U
I	8	21	V
J	9	22	W
K	10	23	X
L	11	24	Y
M	12	25	Z
N	13	0	A
O	14	1	B
P	15	2	C
Q	16	3	D
R	17	4	E
S	18	5	F
T	19	6	G
U	20	7	H
V	21	8	I
W	22	9	J

- A (0) of course
- 13+13=26=>0 (A)
- 13+14=27=>1 (B)
- …

Caesar Cipher

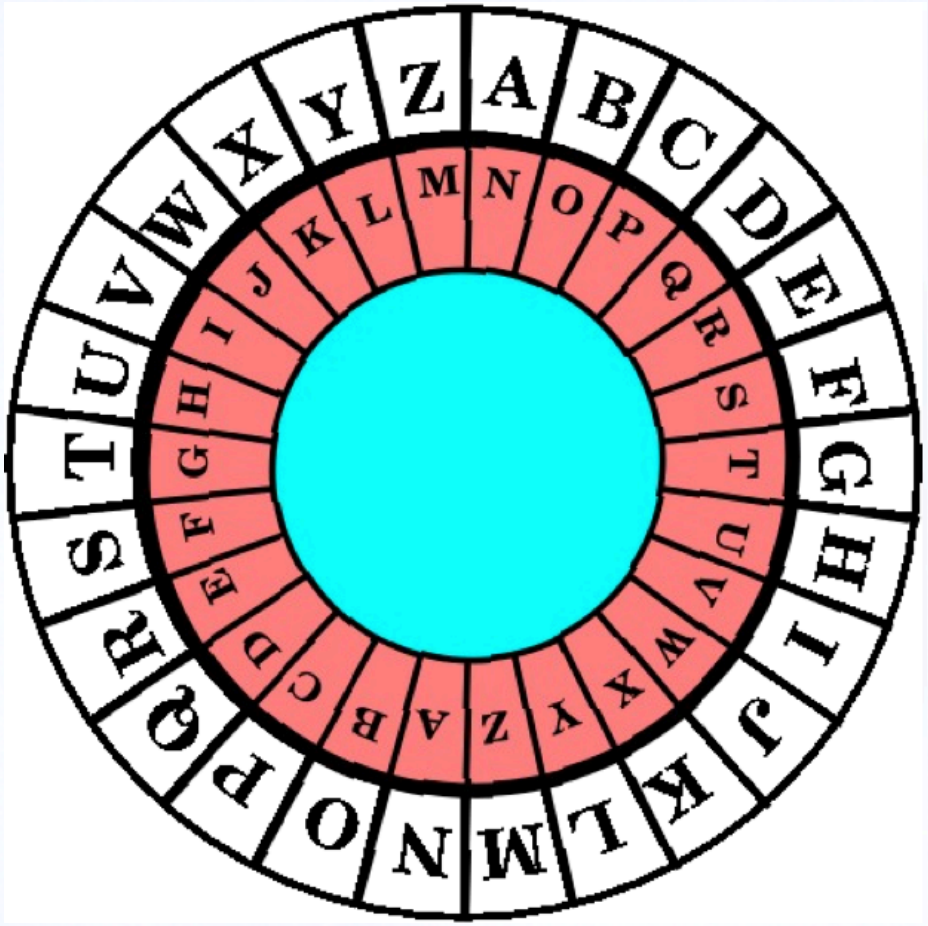


CYBER DISCOVERY

Caesar Cipher

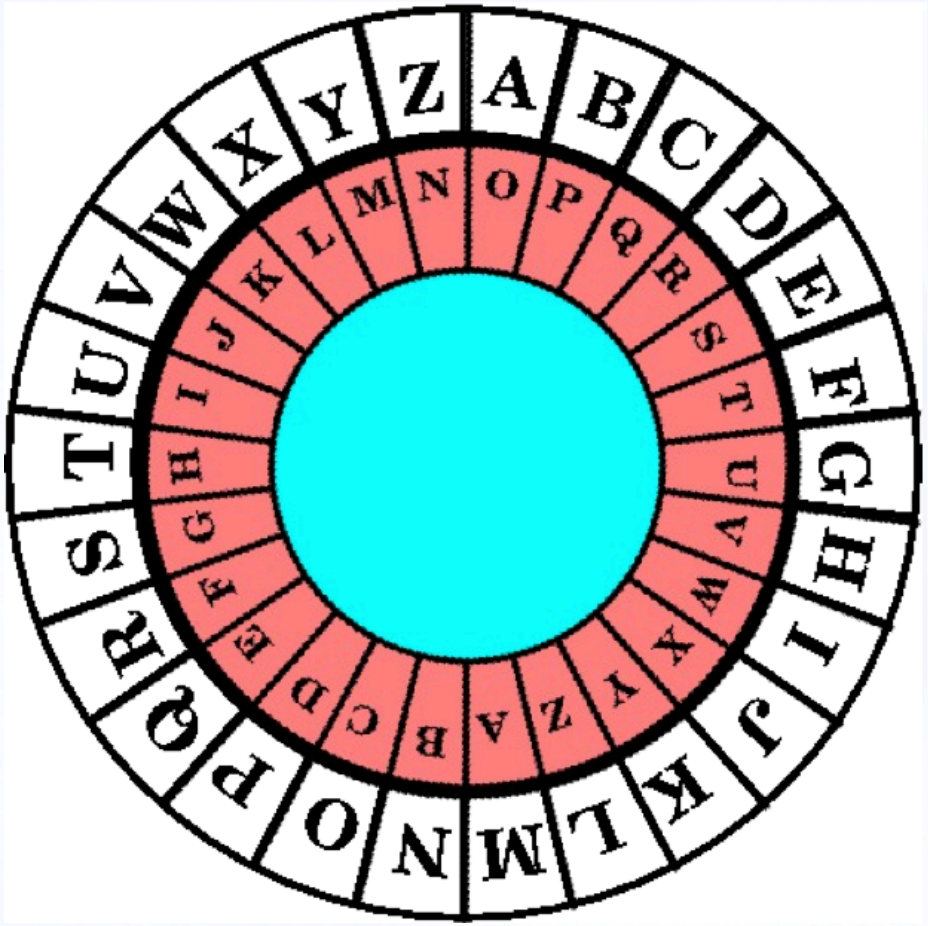
- Nice and simple but not very strong
  - There are only 25 different encryptions

Caesar Cipher

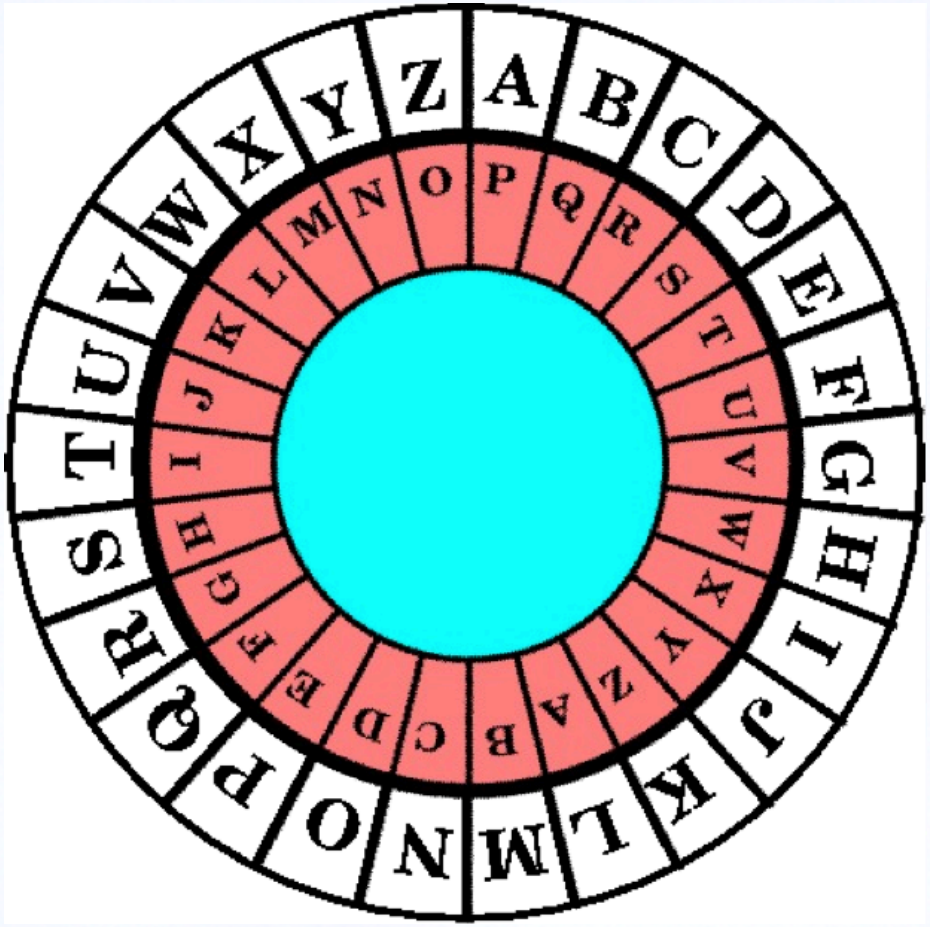


CYBER DISCOVERY

Caesar Cipher



Caesar Cipher



Vigenère Cipher

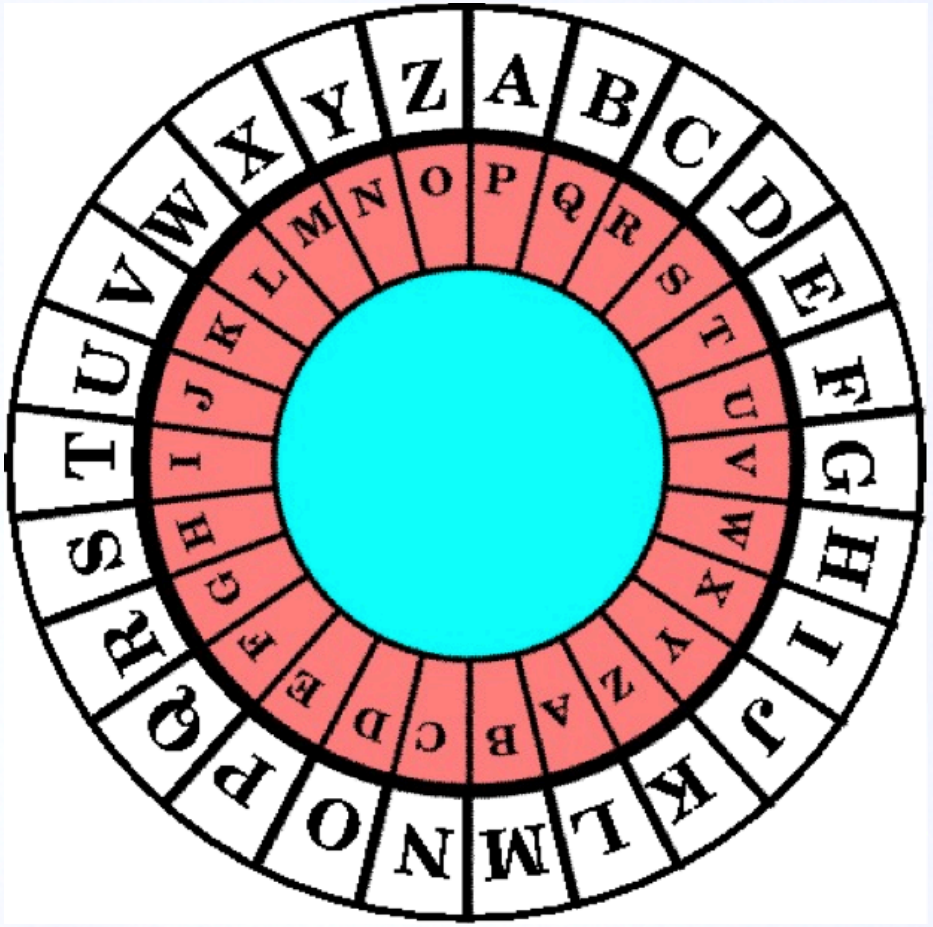
Vigenère Cipher

- Use *different* shift for each letter
- One-time pad: Pattern of shifting *never* repeats
  - 13, 10, 4, 1, 6, 5, 13, 2, 6, 1, 5, 0, 8
- More practical: Use long but known pattern (the key)
  - 15, 0, 18, 18, 22, 14, 17, 3
- Key is best remembered as password
  - P(15), A(0), S(18), S(18), W(22), O(14), R(17), D(3)

CYBER DISCOVERY

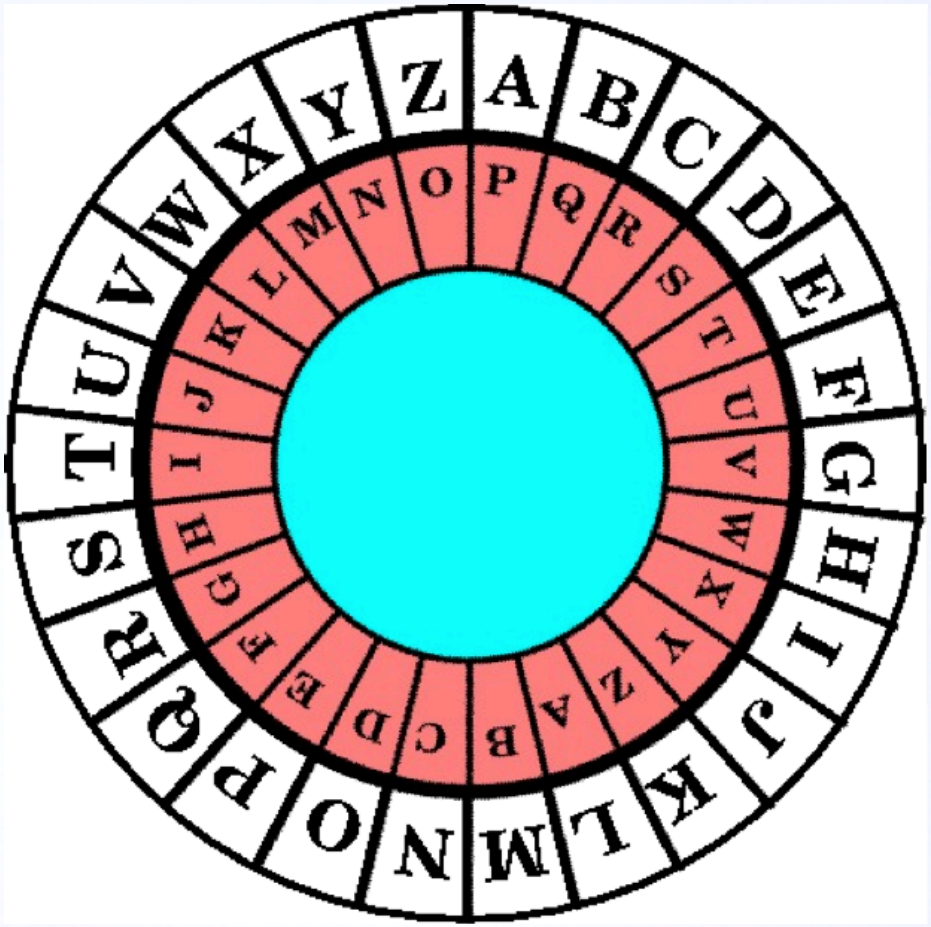
Vigenère Cipher

T	P	
H	A	
E	S	
B	S	
R	W	
I	O	
T	R	
I	D	
S	P	
H	A	
A	S	
R	S	
E	W	
C	O	
O	R	
M	D	
I	P	
N	A	
G	S	



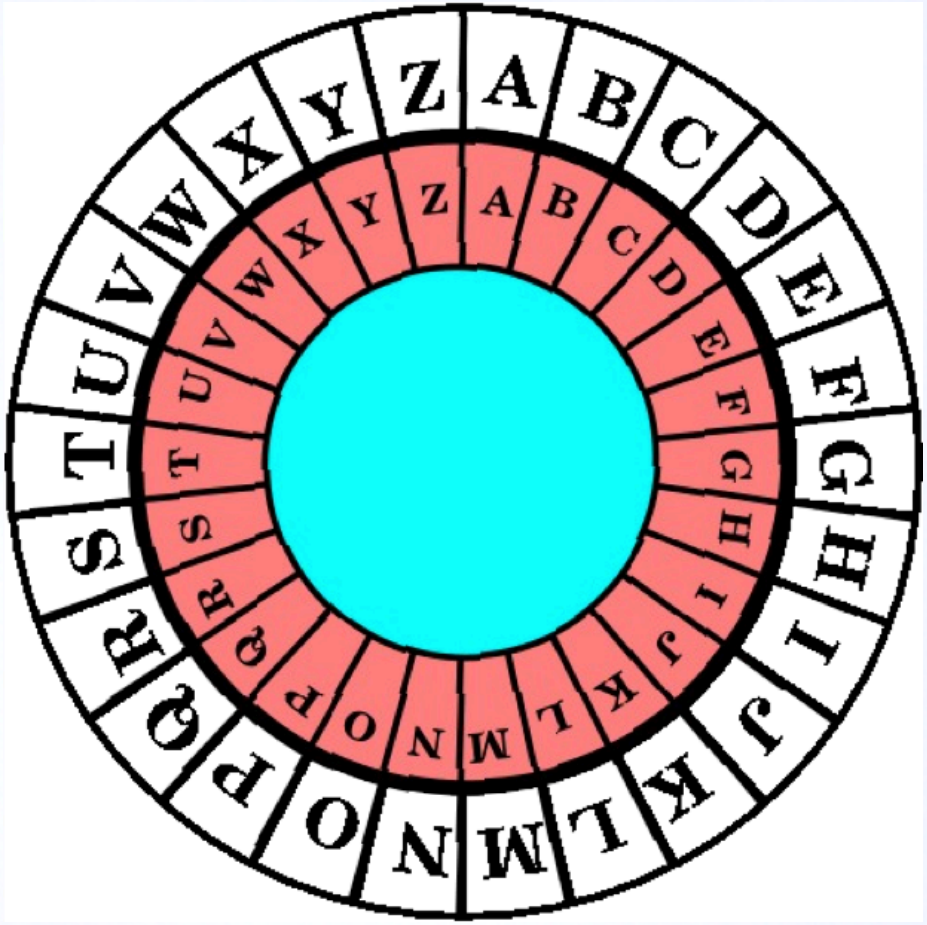
Vigenère Cipher

T	P	I
H	A	
E	S	
B	S	
R	W	
I	O	
T	R	
I	D	
S	P	
H	A	
A	S	
R	S	
E	W	
C	O	
O	R	
M	D	
I	P	
N	A	
G	S	



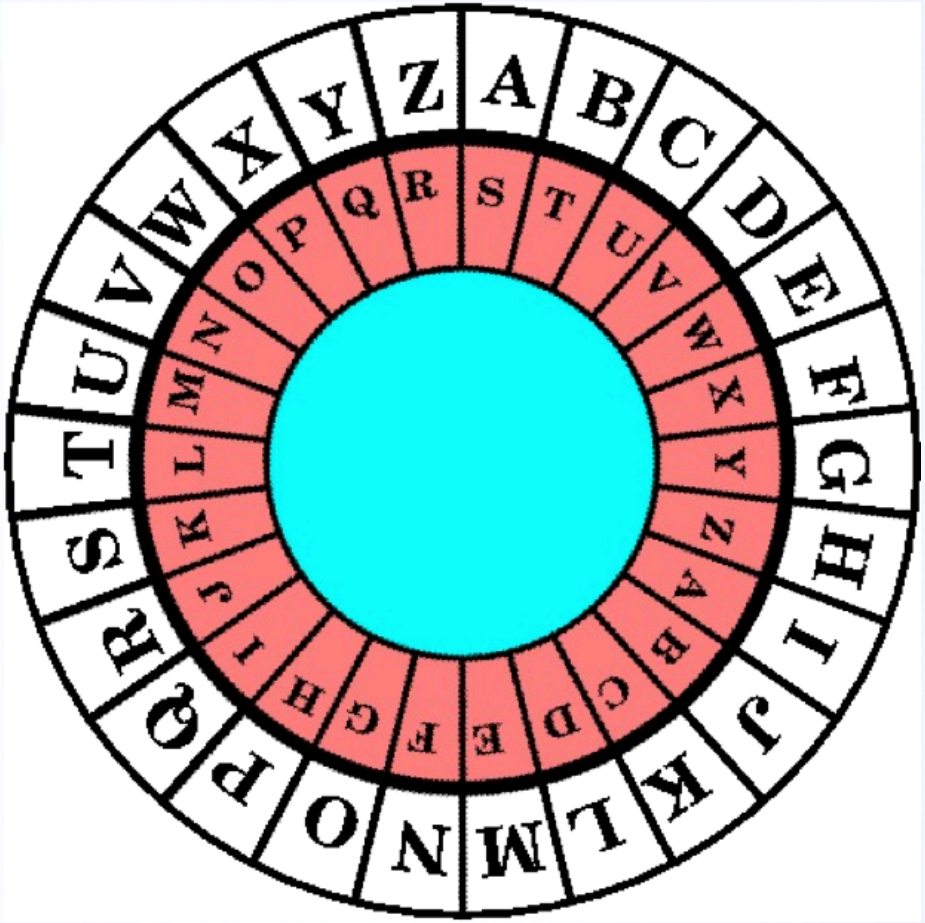
Vigenère Cipher

T	P	I
H	A	H
E	S	
B	S	
R	W	
I	O	
T	R	
I	D	
S	P	
H	A	
A	S	
R	S	
E	W	
C	O	
O	R	
M	D	
I	P	
N	A	
G	S	



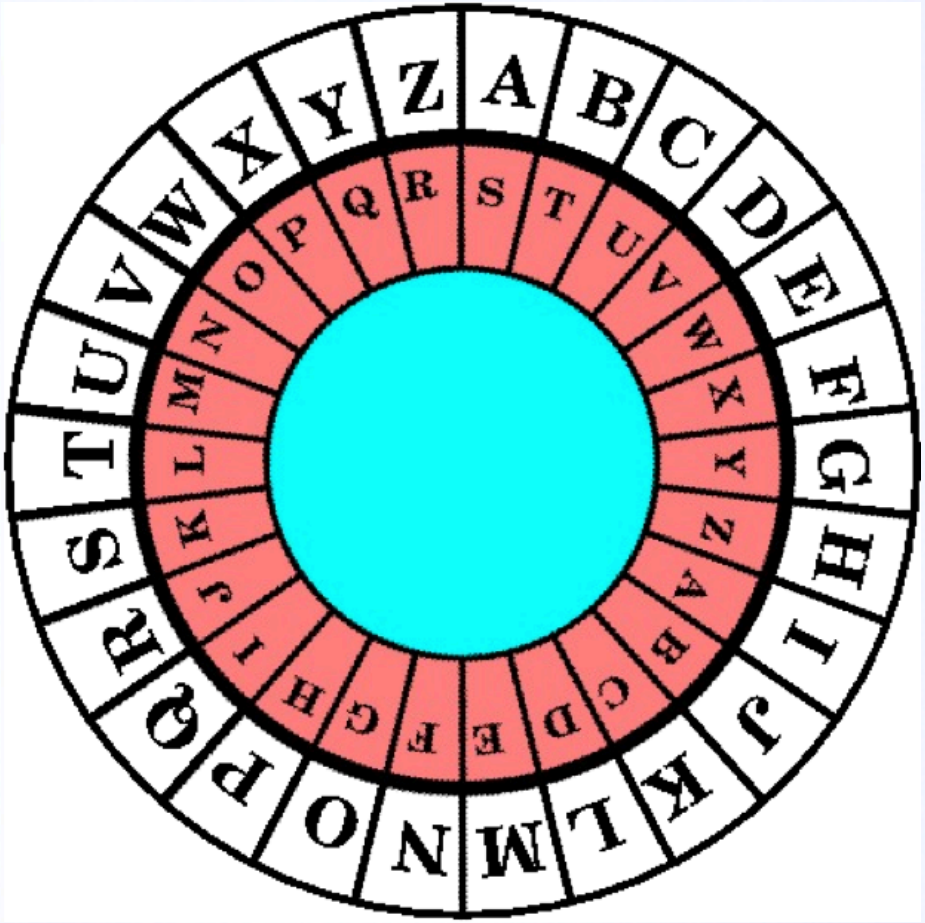
Vigenère Cipher

T	P	I
H	A	H
E	S	W
B	S	
R	W	
I	O	
T	R	
I	D	
S	P	
H	A	
A	S	
R	S	
E	W	
C	O	
O	R	
M	D	
I	P	
N	A	
G	S	



Vigenère Cipher

T	P	I
H	A	H
E	S	W
B	S	T
R	W	N
I	O	W
T	R	K
I	D	L
S	P	H
H	A	H
A	S	S
R	S	J
E	W	A
C	O	Q
O	R	F
M	D	P
I	P	X
N	A	N
G	S	Y



Decipher

- Password: ARTICHOKE
- Text:

TIR IPK TKML,

SNB PLJOV FRBT VV HBC.

Investigative Challenge 2

Tonight, after movie.

Bring your laptops with the Cyber Discovery Toolkit.

CYBER DISCOVERY