Cool stuff learned from the Department of Defense Cyber Crime Digital Forensic Challenge (2006)

David C. Smith, CISSP CISM

Georgetown University

with contributions from Mike McDonanld, *The Professionals" (3rd Place Team, Florida State University)*

A little bit about me..

- Information Security Professional, in IT over 18 years, mostly as a consultant in some capacity.
- Work at GU, have a small consulting company – HCP Forensic Services
  - http://www.hcp-fs.com
- B.S. Computer Science, working toward my masters in IA.

Team Hoya Haxa!

- DC3 limits the teams to 4.
  - Mickey Lasky, Sr. Security Analyst
  - Trent Beckett, Security Analyst
  - Jon Hesson, Security Intern
  - David Smith
  - Almost all off-hours, team lunches on me.
- Most of us have 2+ years of digital forensic work & investigations.
- We thought it would be cool to learn something new & develop existing skillz.
- Hoya Haxa?

DC3 Challenge

- DC3 = Department of Defense Cyber Crime Center
  - Defense Cyber Crime Institute
  - Defense Computer Forensics Laboratory
  - Defense Cyber Investigations Training Academy
- RDT&E – Research, Development, Testing, and Evaluation.
- This challenge – Cheap R&D?
- We heard about this challenge from a Slashdot article and a follow-up in Network World.

DC3 Challenge (now called the 2006 Challenge)

- Quick breakdown of the competitors
  - Academic, 61 entries.
  - Civilian, 25 entries.
  - Commercial, 21 entries.
  - Government, 7 entries.
  - Military, 6 entries.
  - Countries represented
    - US, Australia, Canada, France, India.
- Total teams 140
- Prize is all expense paid trip to DC3 Conference + bragging rights!

DC3 Challenge

- 01 August 2006: Registration Began.
- 01 September 2006: Challenges Sent.
- 01 December 2006: Last Day to Submit.
- 15 December 2006: Winning Team Announced.
- 21-26 January 2007: DoD Cyber Crime Conference (Prize).
  - So, basically we got 3 months to knock these challenges out!

Rules of Engagement

- After the challenge registrations ballooned to 140, DC3 changes the rules to the first 100 submitted solutions are eligible to win.
- Must submit solutions in DC3 report format to receive credit.
- You do not have complete all challenges, submit what you have completed.
- Commercial tools can be used, copies of created tools must be submitted (exe).
- Secret Bonus is out there, somewhere.

Challenges

- 10 Challenges, plus secret challenge.
  - Media Recovery
    - CD in 2 pieces (1000), floppy disk in 2 pieces (300).
  - Data Carving on a Linux LVM (250).
  - Data Acquisition, Boot a DD image (250).
  - Data Acquisition, Boot a split DD image (500).
  - Image Analysis, Real or CG (200).
  - Keylog cracking (250).
  - Password cracking (250).
  - Steganography using S-tools (200).
  - Audio Steganography (250).

DC3 Digital Forensic Challenge

- Media Recovery: Compact-disc
  - Examiners must develop and document a methodology used to recover data from a damaged compact-disc. You will be expected to **recover a piece of known data from the CD**. Points will be awarded for successfully extracting data from the compact-disc.
  - **Total Weighted Points: 1000**

DC3 – Damaged Media CD

- 44% got full points (11 in 25).
  - Top 11 teams got 100 points.
- No partial points given or available.
  - Top 5 Scoring
    - AccessData, 0x28 Thieves, Professionals, Hoya Haxa, Hacker Factor, SRS, CodeMonkeys, NUCIA, DFAT, Backbone Security, Pirate

DC3 – Damaged Media CD

- 1st challenge to fall - on the first day!
- We split CDs and tested, tested, tested.







DC3 – Damaged Media CD

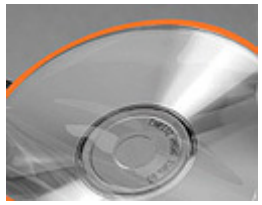
- SA Mickey Lasky discovered D-Skins.
  - http://www.d-skin.com/



  - Snap It On:



  - Leave It On:





DC3 – Damaged Media CD

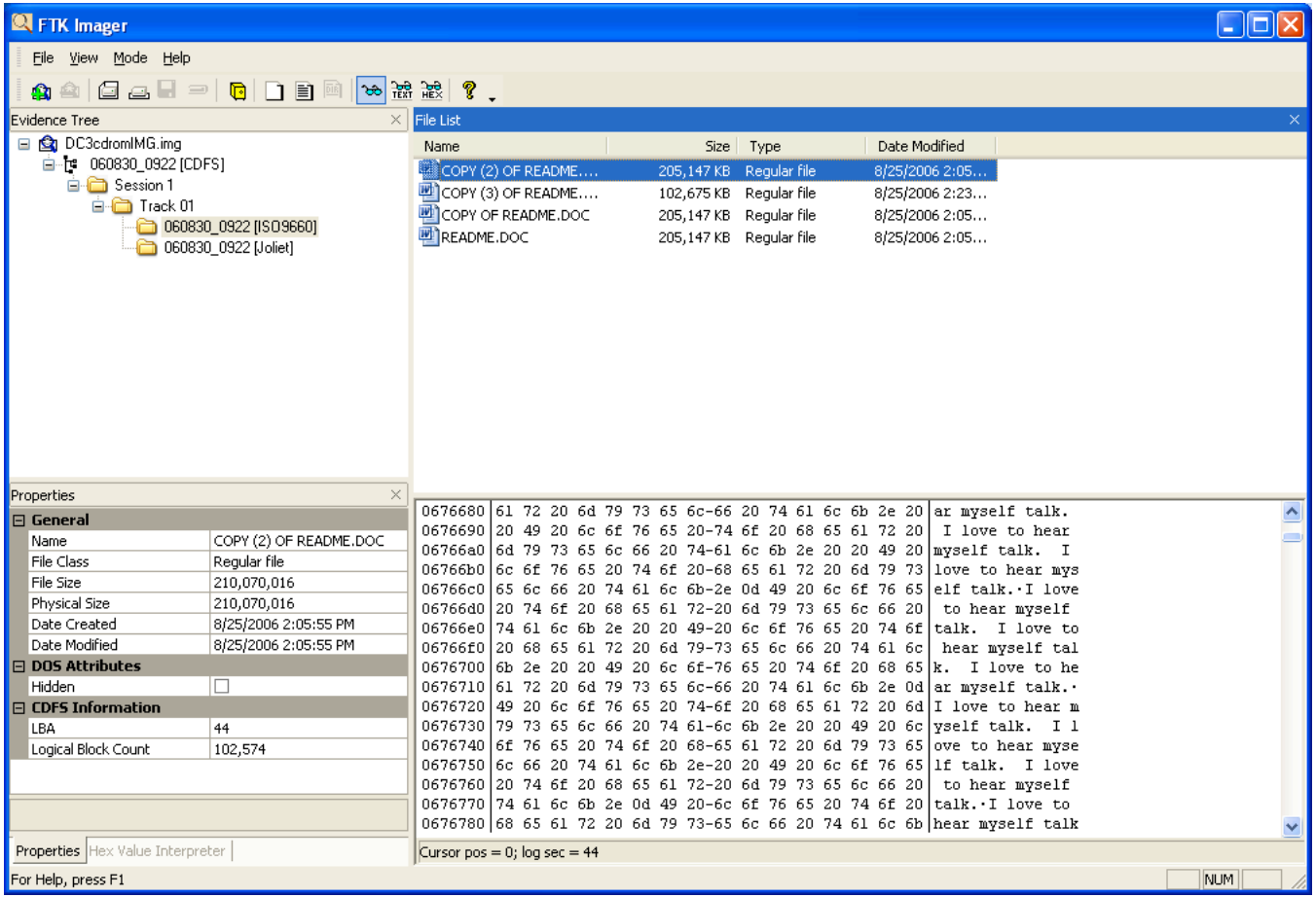
- A little tape – and ready to be read.



This looks beat up – but it looked better when we started.

DC3 – Damaged Media CD

- We read the disk to 11MB (the split).



DC3 Digital Forensic Challenge

- Media Recovery: Floppy Diskette
  - Examiners must develop and document a methodology used to recover data from a damaged floppy diskette. You will be expected to **recover a piece of known data from the floppy**. Points will be awarded for successfully extracting data from floppy diskette.
  - Total Weighted Points: 300

DC3 – Damaged Media Floppy

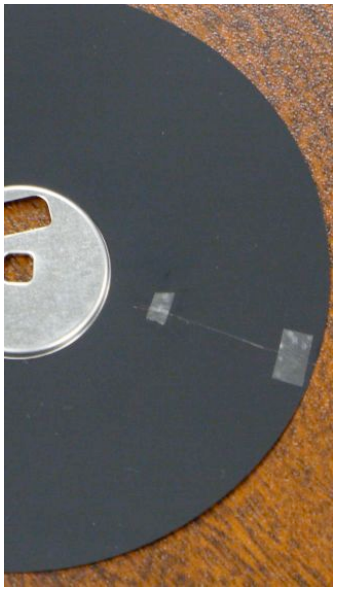
- 20% got full points (5 in 25).
  - Top 4 teams, plus the 6th place finisher got 300.
- No partial points given or available.

  - Top 5 Scoring
    - AccessData, 0x28 Thieves, Professionals, Hoya Haxa,

DC3 – Damaged Media Floppy

- Similar work-up as CD. We carefully examined the evidence floppy and started testing.



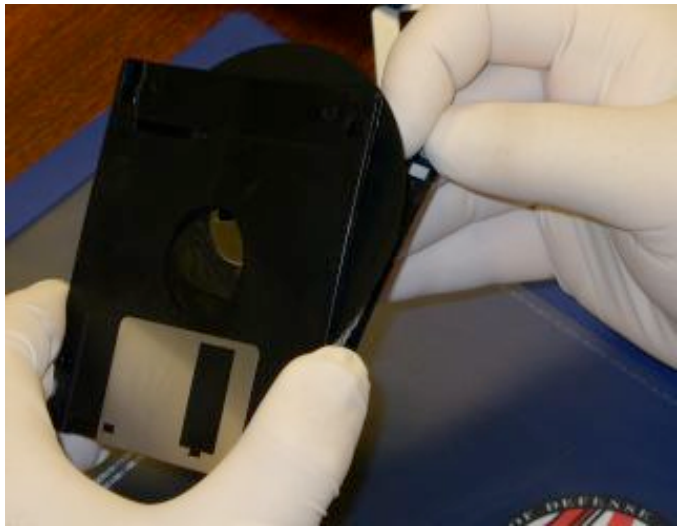


DC3 – Damaged Media Floppy

- We must have tried 20+ methods:
  - Tape
    - One side / both sides [small pics of tape]
    - Thin strips.
    - Only on the edges.
  - Superglue
    - Carefully smooth the superglue on the cut.
  - Nail Polish
    - Carefully applied.

DC3 – Damaged Media Floppy

- Our best results were with very thin strips of film splicing tape on one side.
- Also, we found it best to open the new media container a little as possible.





DC3 – Damaged Media Floppy

- Our old friend:
  - `dd -if=/dev/hdc -of=dc3floppy.img conv=noerror, sync`
- Secret message was "Jack Bauer is my hero!".

DC3 Digital Forensic Challenge

- Data Acquisition - Boot a DD Image
  - Examiners must develop and document a methodology for **booting a dd image without reconstructing the media with normal conventions**. A dd image can be found in the dd Image folder. You will be expected to develop a method to conduct a **live analysis of a dd image by booting the dd image as if it was the local partition housing the bootable operating system**. Points will be awarded for your proof of analysis by means of your methodology.

  - **Total Weighted Points: 250**

DC3 - Boot a DD Image

- 16% got full points (4 in 25).
  - First, fourth, fifth, and 19th place scored 250 points.
- 20% got partial points (5 in 25).
  - 5 teams got 125 points of 250 (50%).
  - Top 5 Scoring
    - AccessData, Hoya Haxa, and Hacker Factor (Dr. Krawetz) got the full points.

DC3 - Boot a DD Image

- Initial analysis show the image to be a partition image, ext3, linux kernel 2.6.
- Understanding the challenge means booting in a VM.
- Identified issues:
  - Partition image needs to be converted to disk image.
  - Partition image does not have MBR / boot manager and can not boot.

DC3 - Boot a DD Image

- First things first
  - Create an image to become our “disk” image.
    - **`qemu-img create disk.img 1G`**
  - Boot up small linux and partition it
    - **`qemu -L . -hda linux.bin -hdb disk.img`**
    - fdisk /dev/hdb
      - n (new), p (primary), 1, [first], [last], w (write)

DC3 - Boot a DD Image

- Boot and migrate from partition to disk
  - **`qemu -L . -hda linux.bin -hdb disk.img -hdc image.dd (challenge dd)`**
- dd from partition to disk
  - **`dd if=/dev/hdc of=/dev/hdb1`**
- Now we have a disk image that is ready to be booted!

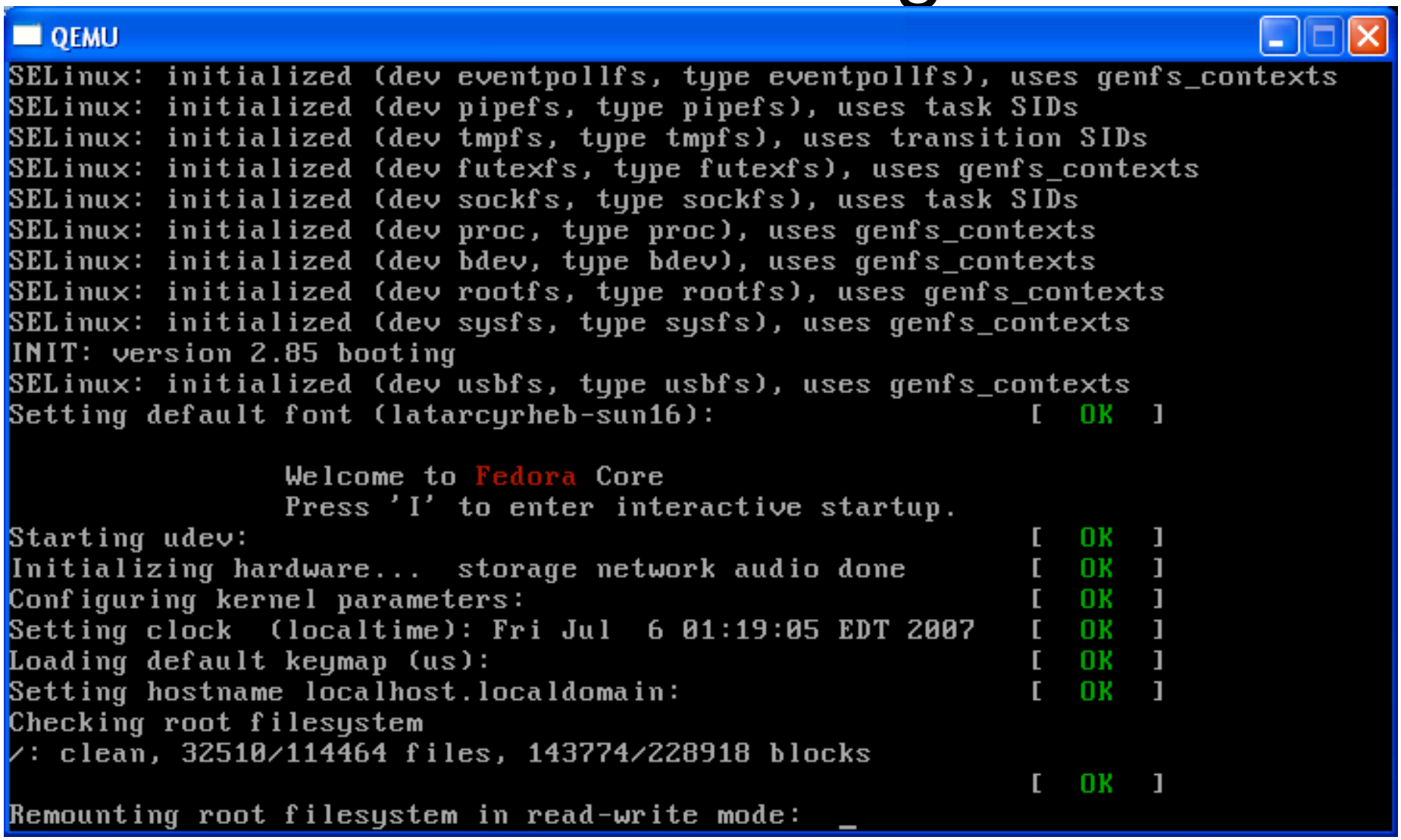
DC3 - Boot a DD Image

- Now I boot to my small version of CentOS that contains GRUB as my 1st disk and our new “disk image”
  - `qemu -L . -hda linux-boot -hdb disk.img`

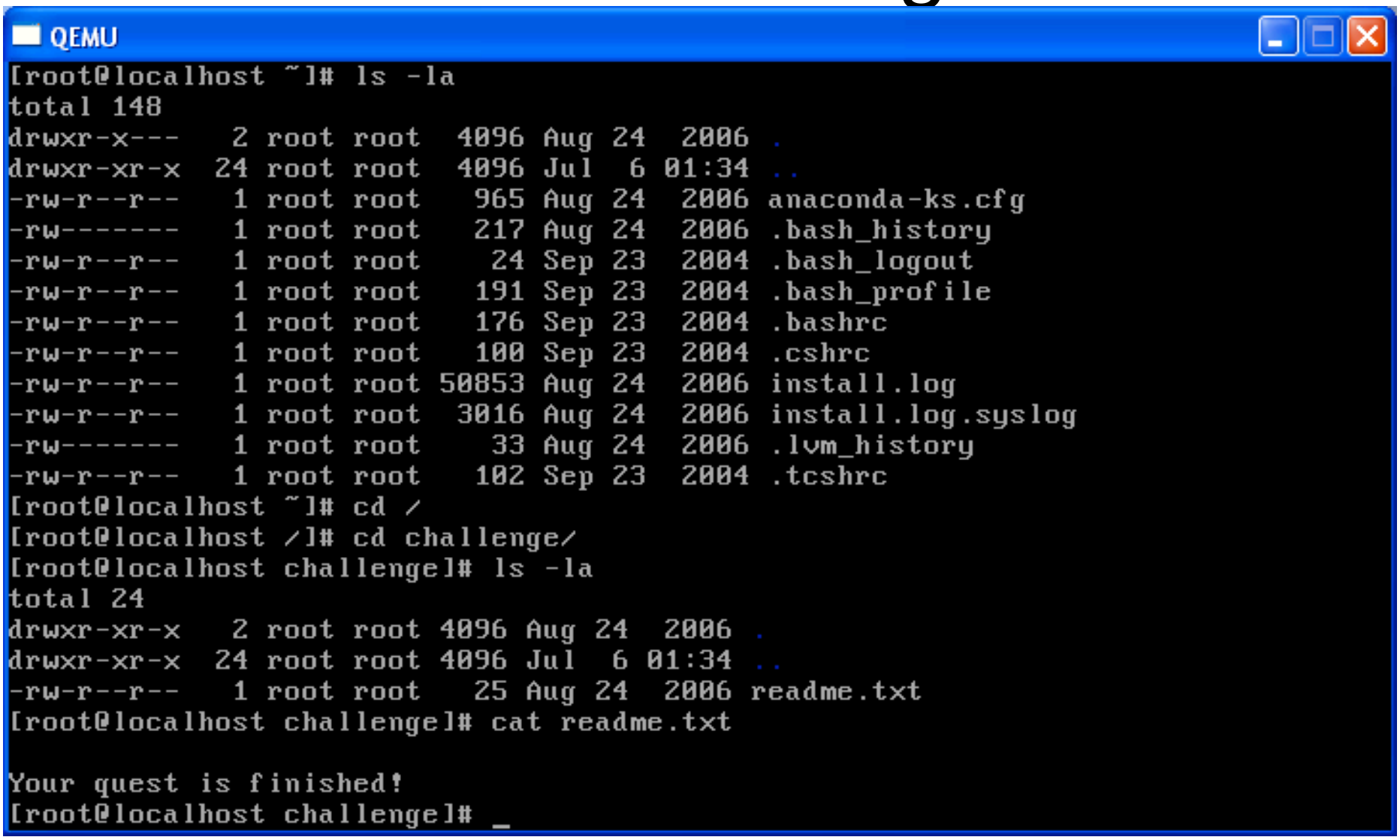
DC3 - Boot a DD Image

- From the GRUB prompt, force the boot to our “disk image”
  - **c for grub command line.**
  - **root (hd1,0) #1st hd, part 0**
  - **kernel /boot/vmlinuz-2.6.9-1.667 root=/dev/hdb1**
  - **initrd /boot/initrd-2.6.9-1.667.img**
  - **boot**

DC3 - Boot a DD Image



DC3 - Boot a DD Image



DC3 Digital Forensic Challenge

- **Data Acquisition: Boot a Split dd Image**
  - Examiners must develop and document a methodology for **booting a split dd image without reconstructing the media with normal conventions.** A split dd image can be found in the Split dd Image folder. You will be expected to develop a method to conduct a **live analysis of a split dd image by booting the split dd image as if it was the local partition housing the bootable operating system. You may not concatenate the slices of the dd image into one piece.** Points will be awarded for your proof of analysis by means of your methodology.
  - **Total Weighted Points: 500**

DC3 – Split DD

- 4% got full points (1 in 25).
  - First place finisher scored 500 points.
- 12% got partial points (3 in 25).
  - 3 teams got 250 points of 500 (50%).
  - Top 5 Scoring
    - AccessData got the 500 points
    - 0x28 Thieves, Professionals, and Hacker Factor (Dr. Krawetz) got 250 points.

DC3 – Split DD

- We did not get any points for this based on my screw-up of the challenge write-up.
- Hoping to get partial points
  - Boot would be similar to boot DD.
  - Combine files in some sort of VM disk configuration file

DC3 – Split DD

- Use VMware VMDK format to combine images into a single virtual drive

```
#######################
### "Boot split DD" ####
#######################
# Extent description
 RW 63 FLAT "mbr.img" 0
 RW 614400 FLAT "image.dd_aa" 0
 RW 614400 FLAT "image.dd_ab" 0
 RW 602560 FLAT "image.dd_ac" 0
 RW 409600 FLAT "buffer.img" 0

 # The Disk Data Base (DDB)
 ddb.adapterType = "ide"
 ddb.geometry.sectors = "32"
 ddb.geometry.heads = "128"
 ddb.geometry.cylinders = "537"
 ddb.geometry.biosSectors = "32"
 ddb.geometry.biosHeads = "128"
 ddb.geometry.biosCylinders = "537"
 ddb.virtualHWVersion = "3"
 ddb.toolsVersion = "0"
```

- Run fdisk to repartition the new disk using evidence gathered from system files
  - /root/anaconda-ks.cfg
  - /etc/fstab
  - /etc/mtab
  - /boot/grub.conf

** Content provided by "The Professionals" (3rd Place Team, Florida State University) **

DC3 Digital Forensic Challenge

- **Data Carving: Linux LVM Interpretation**
  - Examiners must develop and document a **methodology used to interpret a Logical Volume Management (LVM) partition.** An image of an LVM partition can be found in the LVM folder. You will be expected to develop a method to effectively analyze and **recover a deleted file from an LVM partition.** Points will be awarded for your proof of analysis by means of your methodology.
  - **Total Weighted Points: 250**

DC3 – Data Carving

- 20% got full points (5 in 25).
  - Top 4 and 6th place finishers got 250 points.
- 8% got partial points (2 in 25).
  - 2 teams got 25 points of 250 (10%).
  - Top 5 Scoring
    - AccessData, 0x28 Thieves, Professionals, Hoya Haxa, SRS (Action Front) all got the full points.

DC3 – Data Carving

- Initial analysis shows that it is indeed an LVM volume.
  - Importing into our forensic viewers (FTK, Autopsy, Encase, WinHex) gave us no OS interpretation.
- Issues identified were
  - Converting a Logical Volume Management partition into a carve-able filesystem.
  - How do we find the files to carve?

DC3 – Data Carving

- It's LVM and you need to process it for deleted files – so you need to "unwrap" it.

- Create a Qemu disk
  - `qemu-img create myimage.img 1G`

- Boot in Qemu with Helix
  - `qemu -L . -cdrom Helix.iso -hdb lvm.dd -hda myimage -boot d`

DC3 – Data Carving

- Find volume and make active
  - **Pvscan**

```
PV /dev/hdb  VG VolGroup00  lvm2 [896.00 MB / 32.00 MB
free] Total: 1 [896.00 MB] / in use: 1 [896.00 MB] / in
no VG: 0 ]
```

  - **Vgchange –ay VolGroup00**

```
1 logical volume(s) in volume group "VolGroup00" now
active
```

DC3 – Data Carving

- Make an image
  - **dd if=/dev/VolGroup00/LogVol00 of=dev/hda**

```
1769472+0 records in
1769472+0 records out
905969664 byes (906 MB) copied 617.905 seconds, 1.5 MB/s
```

- Now we see it as ext3 filesystem
  - 2 folders, root and Lost+Found

DC3 – Data Carving

- Root sector (physical sector 4408) contained:
  - `020000000c0001022e0000002000000c0002022e2e000`
    `00b000000e80f0a026c6f73742b666f756e6400000c0000`
    `0018000f012e726561646d652e7478742e737770000d000`
    `000bc0f0a01726561646d652e747874742e0e000000a80f`
    `0f012e726561646d652e7478742e73777800`

- **Sorry – text, please**

DC3 – Data Carving

- Root sector (physical sector 4408) contained our next lead, the names of deleted files:
  - ```
    ....................
    ......lost+found.. ........readme.txt.swp.
     ......readme.txtt..........readme.txt.swx.................
    ```
- Running down the wrong path, like I seem to do often – this is a data carving challenge – so…
  - Data carving means Scalpel (foremost), reading up on magic recovery and FTtimes.
    ```

DC3 – Data Carving

- Lots of files – no help, sifting through all files found with all signatures on.
- Then it hits me! **.readme.txt.swp**
- Scour the Internet for the magic of vi/vim swap files.
- Look high and low for the format of vi/vim swap files.

DC3 – Data Carving

- No real luck - so I just created one myself!
  - `vi readme.txt`
  - `kill `pidof vi``
- Read the file in hex and the magic is:
  - `62 30 56 49 4D 20 36 2E 33`
  - `b 0 V I M 6 . 3`

DC3 – Data Carving

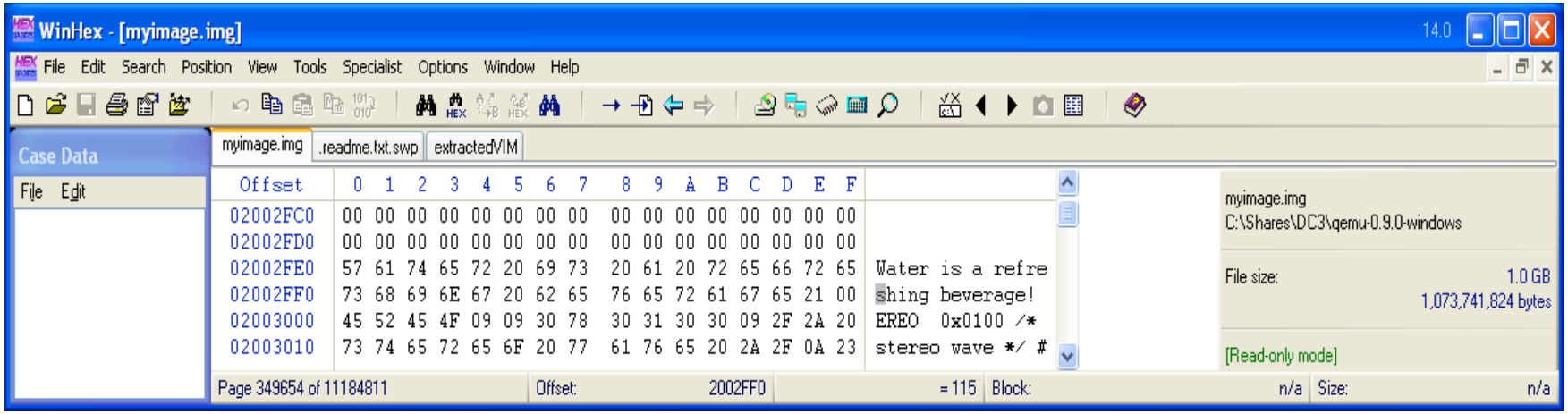
- Not wanting to miss on version, I choose
  - **`62 30 56 49 4D (b0VIM)`**
  - Got 4 hits!
    - **Root /home/readme.txt**
    - Root /etc/mail.helpfile
    - Root /test/readme.txt
    - Root: /boot/grub/menu.lst

DC3 – Data Carving

- Challenge solved:
  - b0VIM 6.3.....$.D...$U..root.....localhost.localdomain...../home/readme.txt....

<snip>

.Water is a refreshing beverage!



DC3 Digital Forensic Challenge

- Metadata Extraction
  - Examiners must develop and document a methodology used to recover the contents of several files. These files will vary in type and the information will be found in several different metadata standards. Clues will be given to help participants know what to look for in each file.
  - Total Weighted Points: 200

DC3 – Metadata Extraction

- Metadata
  - Data about data – information about data.
  - Yes, you can be data and metadata at the same time.
- The challenge – 13 files and 23 questions.
- 5 .jpg, 1 .gif, 1 .eps, 1 .raw, 1 mp3, 1 .mov, 1 .wav, 1 .ra.

DC3 – Metadata Extraction



DC3 – Metadata Extraction

61 metadata datums found!

Make	RICOH
Model	Caplio Pro G3
Orientation	Top, left side
Date/Time	2003:11:13 15:53:45
X Resolution	1/72 inches
Y Resolution	1/72 inches
Resolution Unit	1/72 inches
YCbCr Positioning	Datum point
Copyright	© by Caplio Pro G3
Exposure Time	1/500 sec
F-Number	F5.5
Aperture Value	F5.7
Focal Length	5.7 mm

GPS Version ID	2222
GPS Latitude Ref	N
GPS Latitude	34”9’40.69
GPS Longitude Ref	W
GPS Longitude	117:15’51.87
GPS Altitude	402 meters
GPS Time-Stamp	19:59:14 UTC
GPS Satellites	27,13,10
GPS Status	Measurement in progress
GPS Speed Ref	Knots
GPS Speed	0
GPS Track Ref	True direction
GPS Map Datum	WGS-84

DC3 – Metadata Extraction

- SA Trent Beckett Googled, Googled, Googled.
  - Primary types of metadata types located
    - ID3 – de facto format for MP3 files.
    - EXIF – Exchange Image File Format, a primary image metadata format
    - TIFF – Tagged Image File Format, image metadata format.
    - OLAP – Business Intelligence metadata
    - XML – Human readable metadata

DC3 – Metadata Extraction

- We looked at many tools, but found a clear winner that was able to identify 12 of 13 files.
  - EXIF extractor written in perl by Phil Harvey.
  - http://owl.phy.queensu.ca/~phil/exiftool/
  - Updated as of 7/6/2007!
  - Supports EXIF, GPS, IPTX, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP, ID3 + more.

DC3 – Metadata Extraction

- Remaining file was the .gif file.
  - Used ImageMagick's identify program.
- Sample questions
  - Q: test9.mp3 - What are the MS stereo and intensity stereo settings?
  - A: MS Stereo = ON, Intensity Stereo = OFF
  - Q: test12.wav - What type of encoding is used?
  - A: Microsoft PCM (Package Command Manager)
  - Q: test1.jpg - What is the dateiname?
  - A: Dateiname (German for file name) is: DSCN1767.JPG

DC3 Digital Forensic Challenge

- Secret Bonus
  - Examiners have an opportunity to discover the “secret bonus” and be awarded additional bonus points. **Clue: “You’ll know it when you see it”**
  - **Total Weighted Points: 300**

DC3 – Secret Bonus

- All or nothing, 36% got full points (9 in 25)
  - AccessData, 0x28 Thieves, Hoya Haxa, Code Monkeys, Factor / Phaktor, Digital Lazarus, rm –rf sobriety, nameless, Diverse Digital Detectives got the 300.
- Top 5 Scoring
  - AccessData, 0x28 Thieves, Hoya Haxa got 300 points.

DC3 – Secret Bonus

- “You will know it when you see it”
- We saw it – right away!







DC3 Digital Forensic Challenge

- It's the binary, of course!
- 0111001001111010011011100111011001111001001000000111000101110000001100
  1100100000011001110111010101110110011001100010000001100110011100 10
  0111000001100101011100010110011100100000011010100110001001100101 01
  1100010011101000100000011101010110100001111010011110100111001001100101

- I like breaking codes, but do not seem to be very good at it – but this one is really easy!

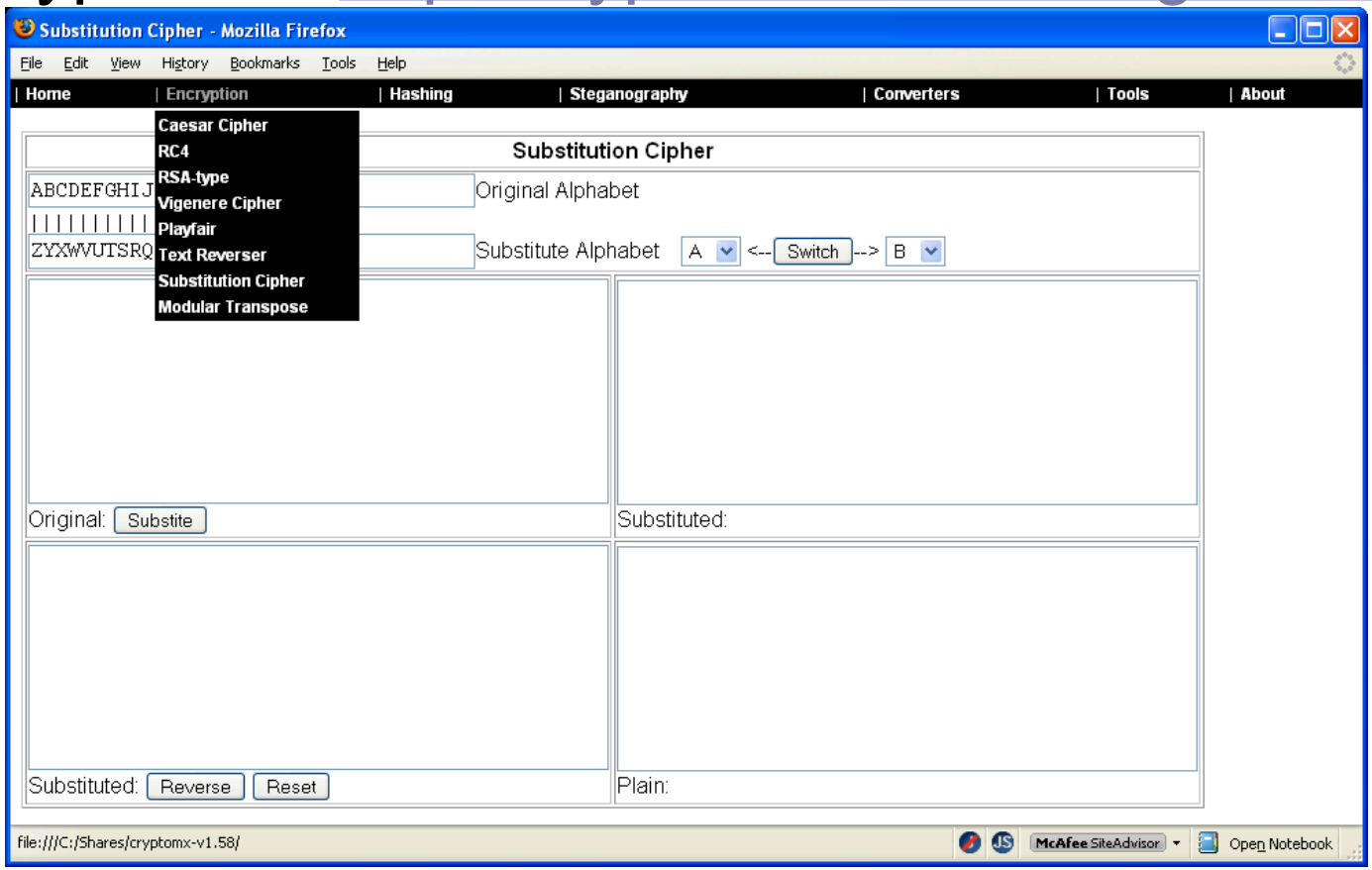
DC3 Digital Forensic Challenge

- Binary to ASCII
- "rznvy qp3 guvf frpeqg jbeq: uhzzre" .

- First thought was:
  - Monoalphabetic = simple substitution.
  - Based on the 3 and “:” + looks.

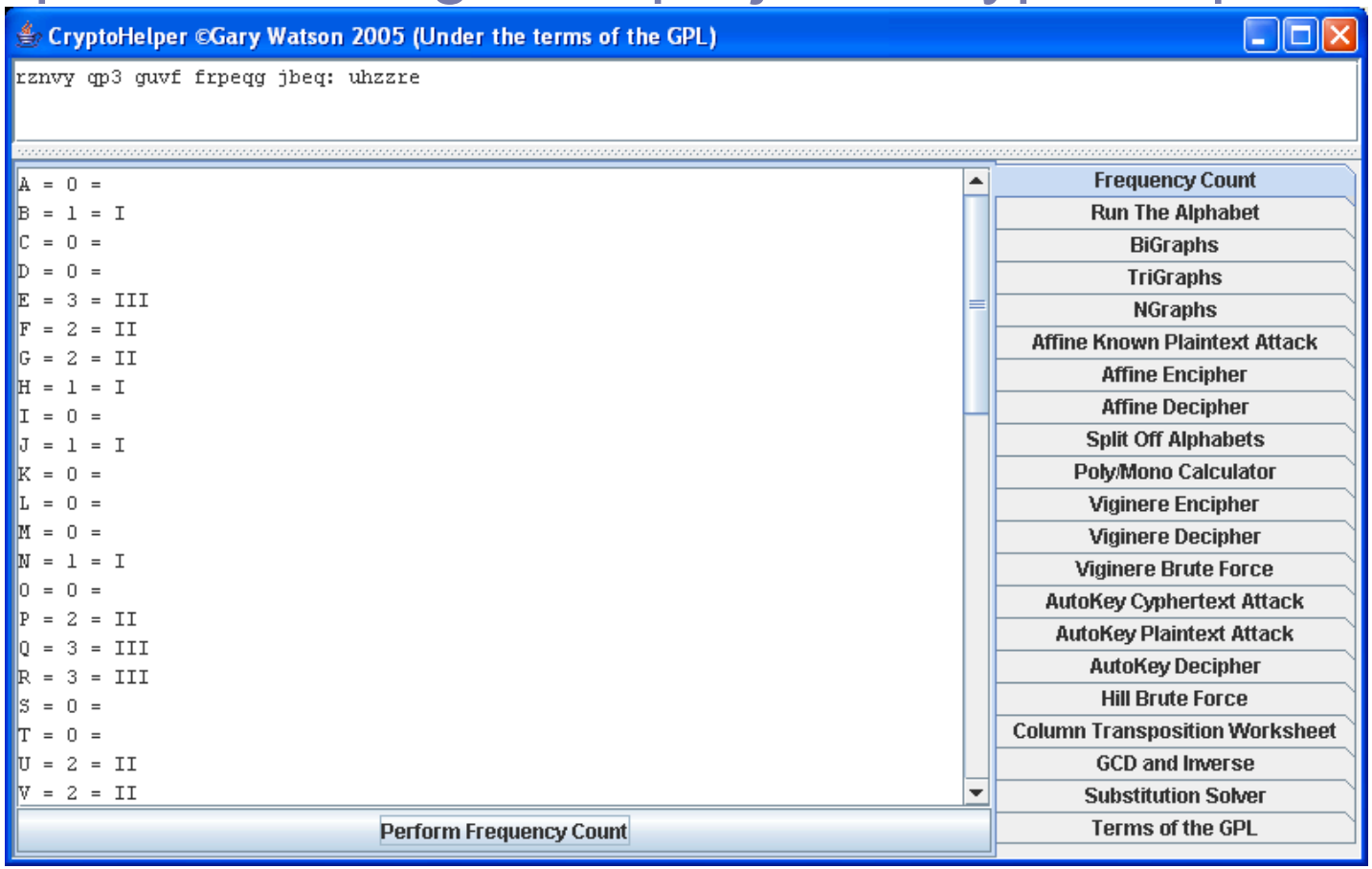
DC3 Digital Forensic Challenge

- Tools I like are:
  - Cryptomx - http://cryptomx.sourceforge.net/



DC3 Digital Forensic Challenge

- CryptoHelper
  http://sourceforge.net/projects/cryptohelper/



DC3 Digital Forensic Challenge

- CryptoMX did the convert from binary.
  - It does a lot more that converting.
  - I used it to break the playfair Shmoocon encryption challenge – after I blew all kinds of time working it on paper.
- CryptoHelper for frequency analysis.
  - Confirmed monoalphabetic
  - Also has a nice feature – “Run the Alphabet”
  - ROT 1-26

DC3 Digital Forensic Challenge

- rznvy qp3 guvf frpeqg jbeq: uhzzre
  - dlzhk cb sghr rdbqcs vnqc gtlldq
  - **email dc3 this secrdt word: hummer**
  - fnbjm ed uijt tfdseu xpse ivnnfs
  - gockn fe vjku ugetfv yqtf jwoogt
  - hpdlo gf wklv vhfugw zrug kxpphu
  - iqemp hg xlmw wigvhx asvh lyqqiv
  - jrfnq ih ymnx xjhwiy btwi mzrrjw
- Oh, ROT13.

DC3 Digital Forensic Challenge

- Keylog Cracking
  - Examiners must develop and document a methodology used to recover the contents of an encrypted keylog file. The keylog file can be found in the Keylog Cracking folder. You will be expected to develop a method to effectively **decrypt and recover the contents of the keylog files**. Points will be awarded for your proof of analysis by means of your methodology.
  - Total Weighted Points: 250

DC3 – Keylog Cracking

- No team got full points!
- 20% got partial points (5 in 25).
  - 4 teams got 200 points of 250 (80%).
  - 1 team got 100 points of 250 (40%).
  - Top 5 Scoring
    - AccessData, 0x28 Thieves, Professionals got 200 points.

DC3 – Keylog Cracking

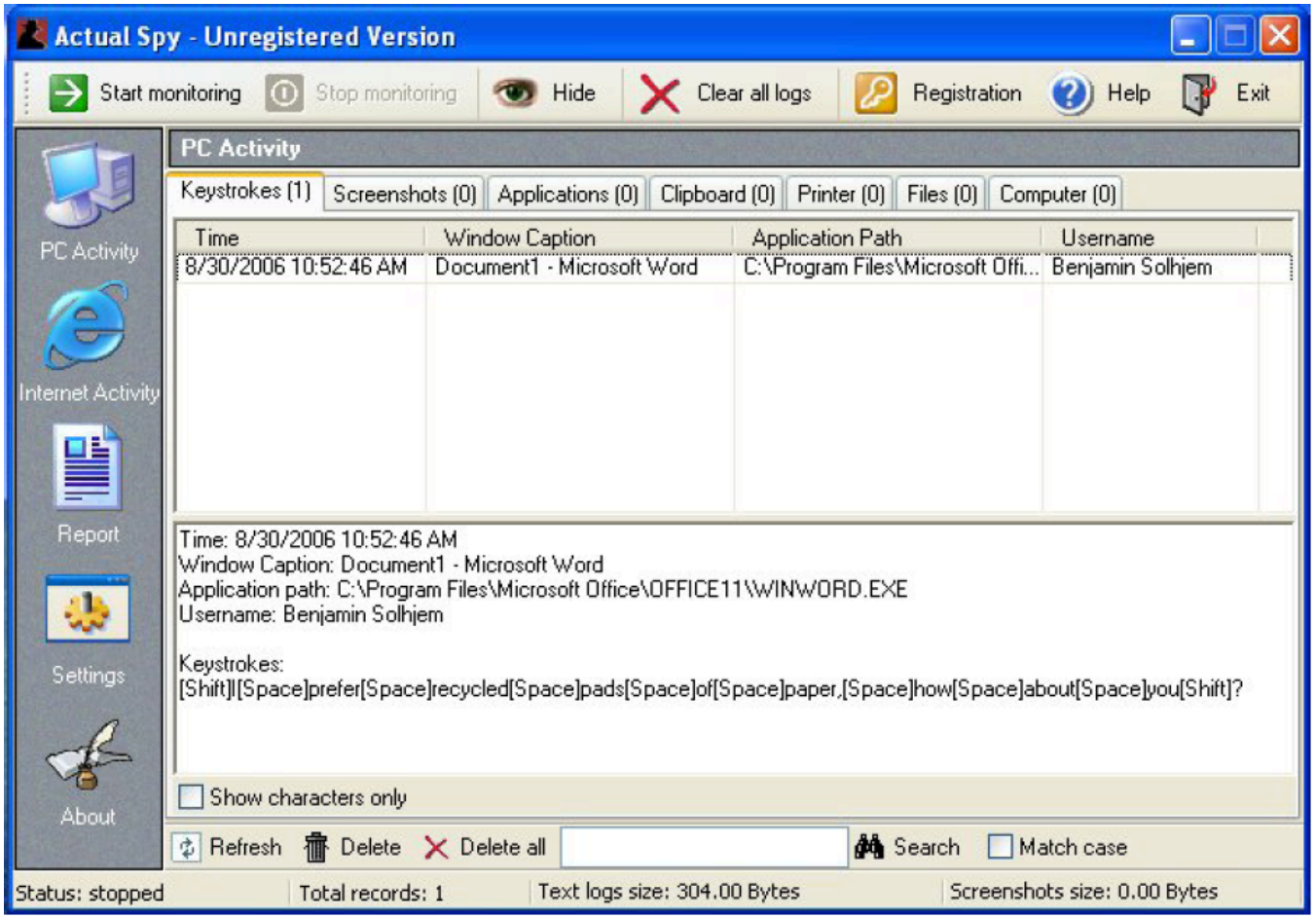
- Hello Google…
  - Search for common key loggers
  - Create sample logs using ~10 apps
- **Actual Spy** logs had striking resemblance to the challenge logs…lets give it a try
- Substitute the encrypted challenge logs into the keyloger's default output path (individually)
- Fire up the application…voila
- Default Settings: encrypt logs w/o password

```
NpfTvZKQKlM8Jh19/vI
/ARPMKb2eRF44gz2Z1CiCNYGqc/QQSBaAyN
4AegLjffTp/lGqeJ96FdQycUuVnHks/clOBBe/zRvd/maHYXT6MSH67/zz/SeHAdXsp0UxQH
5wcOTDTBCvravg38jtv1wA
gMNgt8ee2lYouZuwSB211clBuEWtT2Lit7uvR6lIfmmyA+UmVau65mF2+pWqWgVOZ2PALHVQCDs3ridgRwRqc92h/
mRFVGSdEyHyxpIHh81hz7TcAVJnoqOLX54fgTTbYz5Yu54/duNSuwOUHB
```

** Content provided by "The Professionals" (3rd Place Team, Florida State University) **

DC3 – Keylog Cracking

- Screen Capture of “keylog1.dat” once decrypted



** Content provided by “The Professionals” (3rd Place Team, Florida State University) **

DC3 Digital Forensic Challenge

- Image Analysis: Real vs. CG
  - Examiners must develop and document a methodology used to determine whether the images in the Image Analysis folder are real or computer-generated (CG). You will be expected to identify the nature of each picture. Points will be awarded for each successfully identified picture provided you supply a detailed methodology of how you derived your conclusion. Points will not be awarded for guessing.
  - Total Weighted Points: 200

DC3 - Image Analysis: Real vs. CG

- No team got full points!
- 24% got partial points (6 in 25).
  - 1 team got 170 points of 250 (68%).
  - 1 team got 150 points of 250 (60%).
  - 1 team got 140 points of 250 (56%).
  - Remaining teams got 80, 70, 55.
  - Top 5 Scoring
    - Professionals got 150, with a really solid methodology.
    - Hacker Factor (Dr. Krawetz) got 80.
  - **Props to Blue Blood Alpha (Penn State, 22 place) for the high score!**

DC3 - Image Analysis: Introduction

- "Real" - images captured by cameras
  - May be altered by digital camera software
  - Scanned in from actual film prints
- "CG" - images created or modified by graphics or photo editing software
  - Adobe Photoshop, Autodesk Maya, etc.

Where do we begin…?

Assume all images are innocent (Real) until proven guilty (CG).

** Content provided by "The Professionals" (3rd Place Team, Florida State University) **

DC3 - Image Analysis: A Challenging Task

- Visual inspection is subjective
  - Important part of overall examination process
  - Human eye instinctively detects real from fake
- Statistical Tests have an advantage
  - Ability to offer unbiased results based on forensically sound and replicable procedures
- Use Hybrid Approach
  - Visual inspection + statistical tests
  - Increases the confidence level in your ability to correctly discriminate Real from CG images

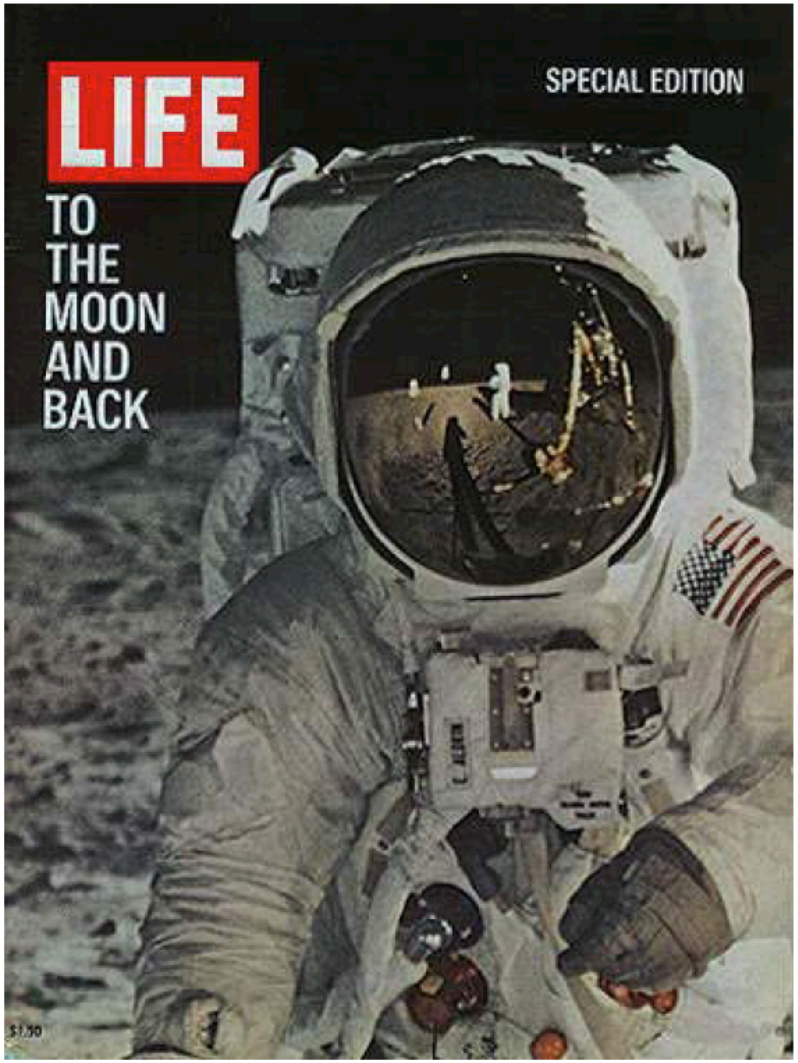
** Content provided by "The Professionals" (3rd Place Team, Florida State University) **

DC3 - Image Analysis: Methodology

- No one method is 100% accurate!
- Each test has different strengths and weaknesses
  - Visual inspection
  - Color frequency histograms
  - Fast Fourier Transforms
  - Metadata
  - Surface Plots
  - Other Individual Tests
  - Other suggested statistical tests
- Cumulative score from each test increases the overall confidence in a final decision

** Content provided by "The Professionals" (3rd Place Team, Florida State University) **

DC3 - Image Analysis: You be the judge…





** Content provided by "The Professionals" (3rd Place Team, Florida State University) **

DC3 Digital Forensic Challenge

- Password Cracking
  - Examiners must develop and document a methodology used to discover the payload of password protected files located in the Password Cracking folder. You will be expected to identify the payload and password for each file. You will find passwords varying in difficulty ranging from 40-bit to 256-bit key strength. Points will be awarded for each piece of information recovered.
  - **Total Weighted Points: 250**

DC3 – Password Cracking

- No team really did well on this challenge
  - Team Hoya Haxa thought it was too much of a serious hardware commitment.
- 28% got partial points (7 in 25).
  - 7 teams got 20 points of 250 (8%).
  - Top 5 Scoring
    - 0x28 Thieves, Professionals got 20 each.
    - Surprise to us, AccessData got a **0**.

DC3 – Password Cracking

- Four Challenge Files
  - DC3ChallengeZip.zip
    - Encryption 256
    - Password H&!!0H0w@reY0ukEo#()h&y
    - 23 letters, 72 letter keyspace
  - DC3ChallengeZip2.zip
    - Encryption 128
    - Password бросать вызов меня

DC3 – Password Cracking

- Four Challenge Files
  - DC3ChallengeZip3.zip
    - Encryption 128
    - Password kEp#()h&y
    - 9 letters, 72 letter keyspace
  - Passwordchinese.doc
    - Encryption 40
    - Password **名词**

DC3 Digital Forensic Challenge

- Steganography using S-Tools
  - Examiners must develop and document a methodology used to determine which files in the Steg Stools folder contain steg. You will also be expected to identify the carrier file and payload, in addition to recovering the password (where applicable) for each file you identify as containing Steganography. Points will be awarded for each successfully accomplished task.
  - Total Weighted Points: 200

DC3 – Steganography using S-Tools

- Not a good turnout on this challenge
  - 24% got partial points (6 in 25).
    - 2 teams got 50 points of 200 (25%).
    - 2 teams got 40 points of 200 (20%).
    - 2 teams got 20 points of 200 (10%).
  - Top 5 Scoring
    - Access data got 40, Professionals got 20.

DC3 Digital Forensic Challenge

- Audio Steganography
  - Examiners must develop and document a methodology used to determine which files in the Steg Audio folder contain steg. You will also be expected to identify the carrier file and payload, in addition to recovering the password (where applicable) for each file you identify as containing Steganography. Points will be awarded for each successfully accomplished task.
  - **Total Weighted Points: 250**

DC3 – Audio Steganography

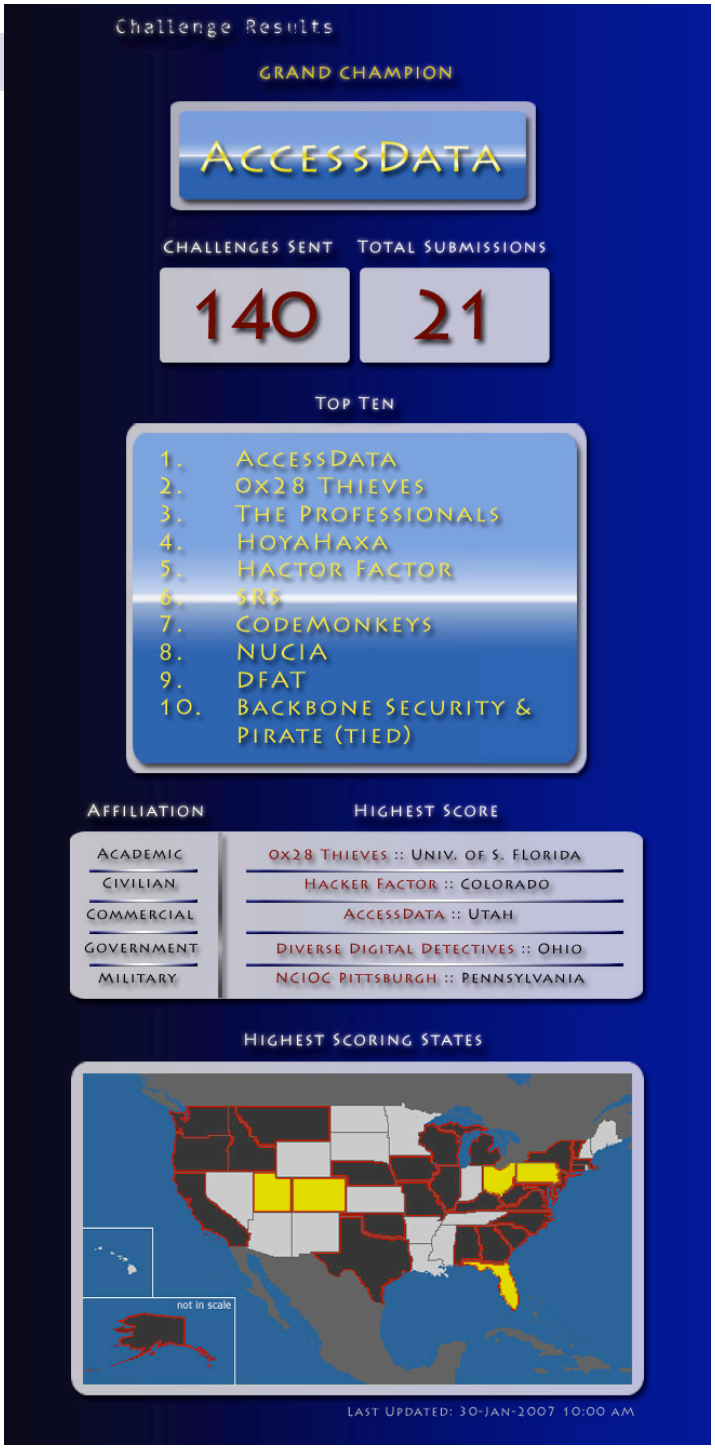
- Not a good turnout either…
  - 12% got partial points (3 in 25).
    - 1 team got 40 points of 250 (16%).
    - 2 teams got 20 points of 250 (8%).
  - Top 5 Scoring
    - Access data got 40, 0x28 Thieves got 20.

DC3 Challenge Results

- Team Hoya Haxa submitted early, wanted to avoid the rush!
- 15 December 2006
  - AccessData announced the Grand Champion!
  - 0x28 Thieves (U of South FLA) announced Academic Champion.
- Message to team:
  - Excellent job, estimated 64.556% complete.

DC3 Challenge Results

- 02 February 2007
  - Top Ten posted.
  - Team Hoya Haxa in 4th!
  - 3rd in Academic ("The Professionals" from FL State).
  - Of the 140 entries, only 21 even submitted.



DC3 Challenge Results

- 03 April 2007
  - Official scores and results – late due to testing all methodologies.

Team	Points (3950)	% Completed	Rank	Steg 200	Audio Steg (250)	Password Crack (250)	Image Analysis (200)
AccessData	3080	78%	1	40	40	0	0
0x28 Thieves	2665	67%	2	0	20	20	0
Professionals	2515	64%	3	20	0	20	150
Hoya Haxa	2300	58%	4	0	0	0	0
Hacker Factor	1750	44%	5	0	0	0	80

DC3 Challenge Results

Teams	Rank	Data Carving LVM (250)	Boot DD Image (250)	Boot Split DD (500)	Media CD (1000)	Media Floppy (300)	Keylog Cracking (250)
AccessData	1	250	250	500	1000	300	200
0x28 Thieves	2	250	125	250	1000	300	200
Professionals	3	250	125	250	1000	300	200
Hoya Haxa	4	250	250	0	1000	300	0
Hacker Factor	5	250	250	0	1000	300	0

DC3 Challenge Results

Teams	Rank	Metadata Extraction (200)	Secret Bonus (300)
AccessData	1	200	300
0x28 Thieves	2	200	300
Professionals	3	200	0
Hoya Haxa	4	200	300
Hacker Factor	5	200	300

DC3 Challenge Results

DC3 Challenge Score Card (Page 1 of 3)	Total Points	Rank	Percentage of all Challenge Completion	Steg - Stools	Steg - Audio	Password Cracking	Image Analysis	Data Craving: LVM	Boot a dd Image	Boot a split dd Image	Media Recovery: CD	Media Recovery: Floppy	Keylog Cracking	Metadata Extraction	Secret Bonus
Total Possible Points	**3950**			**200**	**250**	**250**	**200**	**250**	**250**	**500**	**1000**	**300**	**250**	**200**	**300**
AccessData (Commerical)	**3080**	**1**	78%	40	40	0	0	250	250	500	1000	300	200	200	300
0x28 Thieves (Univ. of S. Florida)	**2665**	**2**	67%	0	20	20	0	250	125	250	1000	300	200	200	300
The Professionals (FSU)	**2515**	**3**	64%	20	0	20	150	250	125	250	1000	300	200	200	0
HoyaHaxa (Georgetown Univ.)	**2300**	**4**	58%	0	0	0	0	250	250	0	1000	300	0	200	300
Hacker Factor (Dr. Krawetz)	**1750**	**5**	44%	0	0	0	80	0	250	250	1000	0	0	170	0
SRS (ActionFront)	**1745**	**6**	44%	0	0	0	0	250	0	0	1000	300	0	195	0
CodeMonkeys (Norwich Univ.)	**1505**	**7**	38%	0	0	20	0	0	0	0	1000	0	0	185	300
NUCIA (Univ. of Omaha)	**1285**	**8**	33%	40	0	20	0	25	0	0	1000	0	0	200	0
DFAT (ManTech)	**1160**	**9**	29%	0	0	0	0	0	0	0	1000	0	0	160	0
Backbone Security (Commerical)	**1000**	**10**	25%	0	0	0	0	0	0	0	1000	0	0	0	0
Pirate (Civilian)	**1000**	**10**	25%	0	0	0	0	0	0	0	1000	0	0	0	0
Factor/Phaktor (Civilian)	**480**	**12**	12%	0	0	0	55	0	125	0	0	0	0	0	300
Digital 49ers (UNC - Charlotte)	**465**	**13**	12%	20	0	20	0	0	125	0	0	0	100	200	0
Not A Big Truck (ManTech)	**415**	**14**	11%	0	0	20	70	0	125	0	0	0	200	0	0
Digital Lazarus (Civilian)	**300**	**15**	8%	0	0	0	0	0	0	0	0	0	0	0	300
rm -rf / sobriety (Univ. of S. Florida)	**300**	**15**	8%	0	0	0	0	0	0	0	0	0	0	0	300
nameless (Civilian)	**300**	**15**	8%	0	0	0	0	0	0	0	0	0	0	0	300
Diverse Digital Detectives (Gov.)	**300**	**15**	8%	0	0	0	0	0	0	0	0	0	0	0	300
Digital Profilers (Iowa St. Univ.)	**295**	**19**	7%	0	0	0	0	0	250	0	0	0	0	45	0
BMT Data Explorers (Academic)	**260**	**20**	7%	50	20	0	0	0	0	0	0	0	0	190	0
N. FLA. (LE)	**260**	**20**	7%	0	0	0	140	0	0	0	0	0	0	120	0
Blue Blood Alpha (Penn. St.)	**235**	**22**	6%	0	0	20	170	25	0	0	0	0	0	20	0
ClintL (Robic Systems, Inc.)	**200**	**23**	5%	0	0	0	0	0	0	0	0	0	0	200	0
NCIOC Pittsburgh (Military)	**50**	**24**	1%	50	0	0	0	0	0	0	0	0	0	0	0
WILCASTAN (OSU)	**0**	**25**	0%	0	0	0	0	0	0	0	0	0	0	0	0

Learned Tips and Tricks

- This is an attempt to share all of the weird tips and tricks we tried and tested.
- Your mileage may very, feel free to shout out what works for you.
- Please, no “heard this works” – First hand knowledge only!

Data Recovery

- CD / DVD with damaged media, use CD labels to keep foil from coming up.
- CD / DVD, we used metallic silver spray paint when we had broken foil with some success.
- HD / CD / DVD, try different drives and OS. You would be amazed that it works without issue on another OS.

Data Recovery

- CD/DVD writers are much better at reading damaged media. We like:
  - CDs, early Lite-on and Plexstor preferred by CDFreaks and data recovery pros.
  - DVD, Plextor 12x and Pioneer 12x (ebay).
- Cleaning your media
  - Try it first, don’t do anything unless it fails.
  - Isopropyl alcohol.
  - Ivory soap and water.

Data Recovery

- Lots of recovery software exists, but we found that if none work if you get “Media Not Found”
- Lots of software exists:
  - Bad Copy pro, ISOBuster, AD Imager, DVDisaster, dd, dd_rescue, Ontrack, …
  - Team was split, ISOBuster, AccessData FTK & Imager, and BadCopy Pro.

Filesystems and mounting

- Ext2/3 drivers for win32
  - http://uranus.it.swin.edu.au/~jn/linux/ext2ifs.htm
  - http://www.fs-driver.org/
- Mount DD in win32
  - http://www.acc.umu.se/~bosse/