Computer Forensics (Digital Forensic)

SUMMER BRIDGE PROGRAM

DR. HWAJUNG LEE
DR. ASHLEY PODHRADSKY
Dr. Prem Uppuluri

Image Source: thecomputerforensics.info

DAY ONE

Who am I?

Image Source: computerforensicsinfo.org

- Dr. Hwajung Lee
  - Professor
    - in the department of **Information Technology**
    - at Radford University
  - Email: hlee3@radford.edu

Sa-rang, Coco, and Emma

Who is your TA?

- Ms. Kara Sutphin

Image Source: racktopsystems.com

Our Plan for This Week

- DAY ONE (Monday)
  - Lecture and TWO activities
    - **Activity One**: Who are you?
    - **Activity Two**: Digital Forensic Cases
- DAY TWO (Tuesday)
  - Lecture and ONE activity
    - **Activity Three**: Acquiring an Image of Evidence Media and Recovering a Deleted File
    - **Capture the Flag Contest**
- DAY THREE (Wednesday)
  - Lecture and THREE activities
    - **Activity Four**: Grabbing Cookies and Passwords with Wireshark
    - **Activity Five**: Encryption and Decryption
    - **Activity Six:** Steganography
    - **Activity Seven:** Digital Photo Scavenger Hunt
- DAY FOUR (Thursday)
    - **Activity Eight**: Preparing the Friday Presentation
    - **Activity Nine:** Field Trip (Tabletop Activity)
- DAY Five (Friday)
    - **Activity Ten**: Preparing the Friday Presentation
    - **Presentation in the closing session**

Activity ONE:
Who are you?

Image Source: newenglandcomputerforensics.com

Activity ONE:
Who are you?

Image Source: newenglandcomputerforensics.com

- What is your name?
- What is your school?
- What is your favorite indoor/outdoor activity?
- What is your favorite time of day/day of the week/month of the year? Why?
- When you have 2 hours of free-time, how do you pass the time?
- What do you expect from this class and Summer Bridge Program?
- Anything else?

In This week, We will talk about…

Image Source: e-crimebureau.com

- What is computer forensics?
- Computer Forensics in the news
- When is computer forensics used?
- History of computer forensics
- Describe how to prepare for computer investigations
- Computer Forensics Example- AccessData FTK Imager, Wireshark, Encryptor & Decryptor

Forensic

- Adj. - “of, relating to, or used in courts of law or public debate or argument"
  - From the Latin term *forensis (forum)*
- Computer Forensics - Exceedingly poor English expression which uses the noun *computer* as an adjective to modify the adjective *forensic* as a noun Source: class note by Rob Guess
- Digital Forensics – still poor English expression
- I think “**Forensic IT**” is a better expression

Understanding Computer Forensics (1)

- **Computer forensics**
  - Involves obtaining and analyzing digital information
  - Investigates data that can be retrieved from a computer's hard disk or other storage media, including tasks of recovering data that users have hidden or deleted and using it as envidence. Evidence can be **inculpatory** ("incriminating") or **exculpatory**

Image Source: en.wikipedia.org

Understanding Computer Forensics (2)

- Types of Evidence
  - Exculpatory
    - Proves Innocence
  - Inculpatory
    - Proves Guilt
  - Tampering
    - Proves Malfeasance or Mishandling

Source: class note by Rob Guess

Understanding Computer Forensics (3)

- **Related Fields**
  - **Network forensics**
    - Yields information about how a perpetrator or an attacker gained access to a network
  - **Data recovery**
    - Recovers information that was deleted by mistake or intentionally
    - Typically you know what you're looking for
  - **Disaster recovery**
    - Uses computer forensics techniques to retrieve information their clients have lost due to natural or man made disaster

Computer Crime

- Computer as an Instrument of Crime
  - Remote System Penetration
  - Instrument of Fraud
  - Used to Deliver Threats / Harassment
  - DoS Attacks
- Computer as a Victim of a Crime
  - System Compromise
- Repository of Evidence Incidental to Crime
  - Contraband Items
  - Electronic Discovery in Civil Litigation

Source: class note by Rob Guess

The Importance of Being Digital

- People live and work in increasingly digital modes
- Nearly every crime now involves some form of digital evidence
- 3~4% of people will commit a crime given the opportunity
- Internet based crime presents a lower overall risk to the offender when compared to "real world" crime
- This naturally encourages criminals to adapt digital modes

Source: class note by Rob Guess

Digital Evidence

- Name some examples of digital evidence
  - _____
  - _____
  - _____
  - _____

Image Source: nacvaquickread.wordpress.com

Source: class note by Rob Guess

Sources of Digital Evidence

- Open Computer Systems
  - PC's, Servers, Etc
- Communication Systems
  - Telecommunications Systems
  - Transient Network (content) Data
  - Non-transient (log) Data
- Embedded Computer Systems
  - PDAs, Cell Phones, iPods, iPhone, Etc

Source: class note by Rob Guess

Crimes Involving Digital Evidence

- Traditional crimes
- Theft of Trade Secrets
- Harassment
- Intrusion Events
- Malicious Code
- Child Pornography
- Inappropriate Use
- Others?

Source: class note by Rob Guess

Activity TWO:
Digital Forensic Cases (1)

- BTK Killer
  - http://precisioncomputerinvestigations.wordpress.com/2010/04/14/how-computer-forensics-solved-the-btk-killer-case/
- Caylee Anthony
  - http://www.christianpost.com/news/casey-anthony-trial-computer-expert-unearths-chloroform-internet-searches-50980/

Activity TWO:
Digital Forensic Cases (2)

- The Dangers of Internet
  - http://precisioncomputerinvestigations.wordpress.com/2010/04/13/the-dangers-of-the-internet/
- Facebook and Skype Forensics
  - Findings of a Facebook Forensic Analysis
    - http://precisioncomputerinvestigations.wordpress.com/2010/03/09/findings-of-a-facebook-analysis/
  - Chat History
    - http://precisioncomputerinvestigations.wordpress.com/tag/skype-forensics/

Activity TWO:
Digital Forensic Cases (3)

- What Computer Forensics Can Do For You
  - http://precisioncomputerinvestigations.wordpress.com/2010/04/08/what-computer-forensics-can-do-for-you/
- Corporate Fraud – A Case Study
  - http://precisioncomputerinvestigations.wordpress.com/2010/03/29/corporate-fraud-a-case-study/
- Corporate Investigation – A Case Study
  - http://precisioncomputerinvestigations.wordpress.com/2010/03/24/corporate-investigation-a-case-study/

DAY TWO

Digital Investigation :Taking a Systematic Approach

- Steps for problem solving
  - Make an initial assessment about the type of case you are investigating
  - Determine the resources you need
  - Obtain and copy an evidence disk drive
  - Identify the risks- Mitigate or minimize the risks
  - Analyze and recover the digital evidence
  - Investigate the data you recover
  - Complete the case report
  - Critique the case

Securing Your Evidence

- Use **evidence bags** to secure and catalog the evidence
- Use computer safe products
  - Antistatic bags
  - Antistatic pads
- Use well padded containers
- Use evidence tape to seal all openings
- Write your initials on tape to prove that evidence has not been tampered with
- Consider computer specific temperature and humidity ranges

Understanding Data Recovery Workstations and Software

- Investigations are conducted on a computer forensics lab (or data-recovery lab)
- Computer forensics and data-recovery are related but different
- **Computer forensics workstation**
  - Specially configured personal computer
  - Loaded with additional bays and forensics software
- To avoid altering the evidence use:
  - Forensics boot disk, Write-blockers devices, Network interface card (NIC), Extra USB ports, FireWire 400/800 ports, SCSI card, Disk editor tool, Text editor tool, Graphics viewer program, Other specialized viewing tools

Sources of File System Evidence

- File Slack
- Free Space - “Unallocated” Clusters
- Deleted Files
- Page File / Swap Partition
- Unpartitioned “Free” Space
- Host Protected Areas

Source: class note by Rob Guess

Understanding Bit-Stream Copies (1)

- **Bit-stream copy**
  - Bit-by-bit copy of the original storage medium
  - Exact copy of the original disk
  - Different from a simple backup copy
    - Backup software only copy known files
    - Backup software cannot copy deleted files, e-mail messages or recover file fragments

Understanding Bit-Stream Copies (2)

- **Bit-stream image**
  - File containing the bit-stream copy of all data on a disk or partition
  - Also known as **forensic copy**

Class Activity THREE:
Acquiring an Image of Evidence Media and Recovering a Deleted File

- First rule of computer forensics
  - Preserve the original evidence
- Conduct your analysis only on a copy of the data
- Use FTK Imager to create a forensic image
  - http://accessdata.com/product-download
  - Your job is to recover data from deleted files

Privacy and Security on the Internet

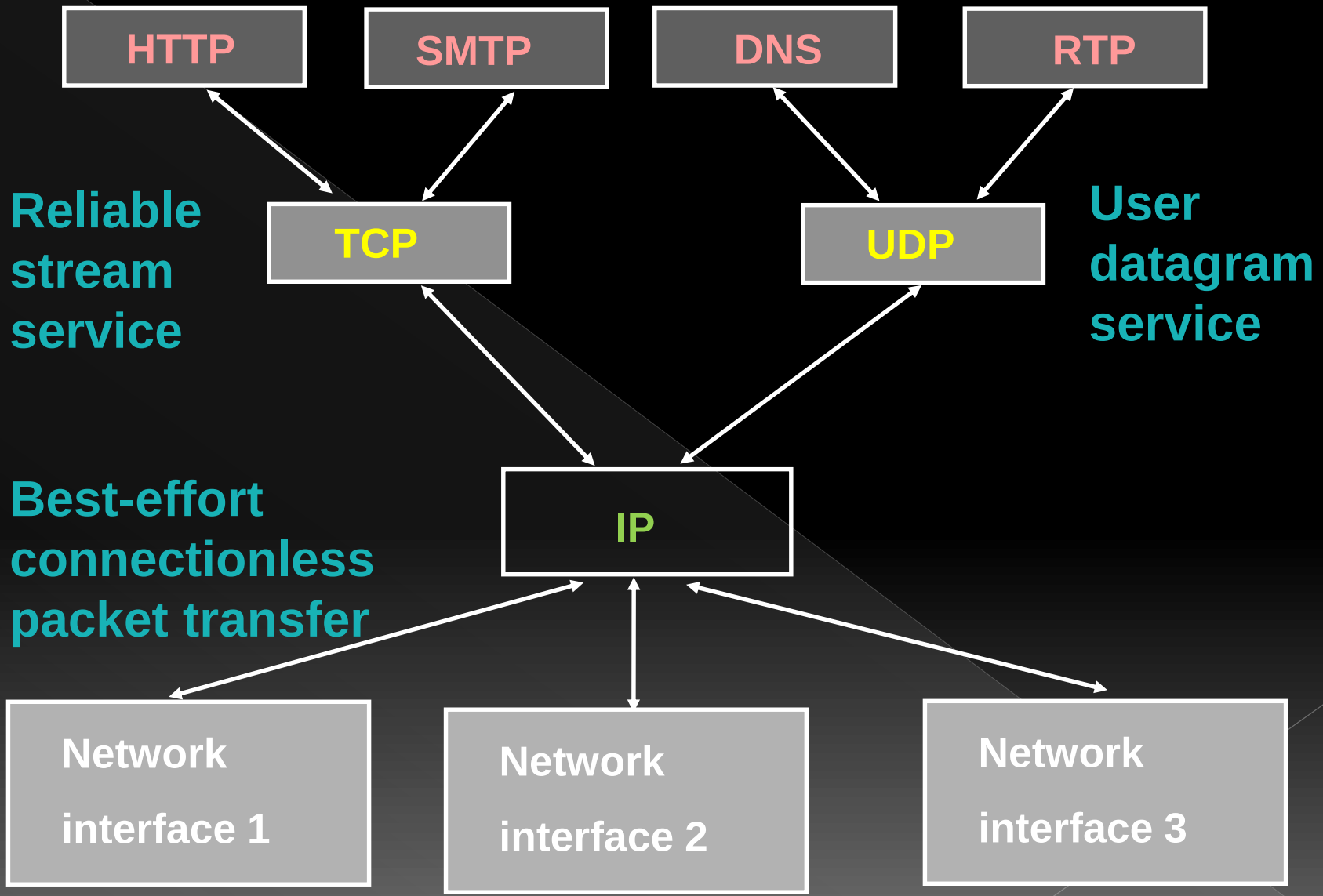
- Privacy on the Internet
  - https://vimeo.com/69216673
    - To watch, enter "security1#"
- Security on the Internet
  - https://vimeo.com/69216833
    - To watch, enter "security1#"

Mini Contest: Capture the Flag Contest

- Instruction:
  - **[Step 1]** Go to: https://137.45.192.119
  - **[Step 2]** Register for an account. You should register as a high school team with a given team name and a given password.
    - Team name: (ex) team1, team2, team3, …
    - Password: (ex) secure1$, secure2$, …
  - **[Step 3]** Once you register and login, you can start working on challenges. You will see your scores on the scoreboard. For reference you can see the scores of other high school students who have competed over the last 4 months.

DAY THREE

TCP/IP Protocol Suite

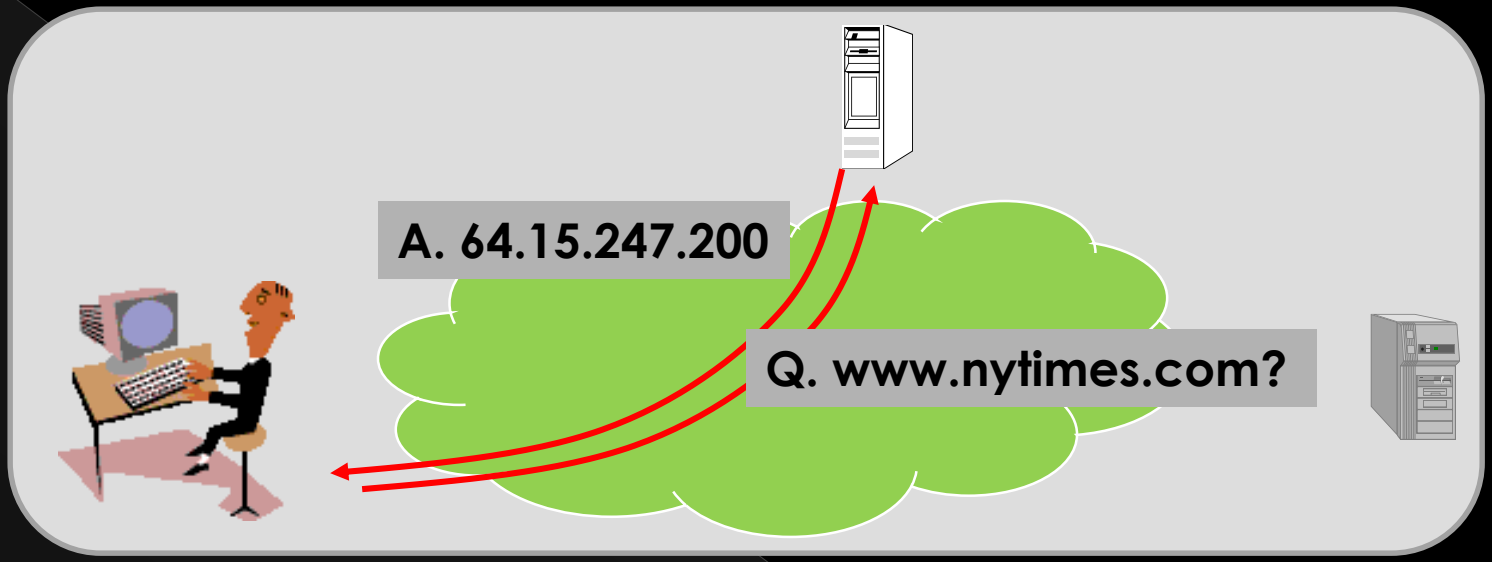


Web Browsing Application

- World Wide Web allows users to access resources (i.e. documents) located in computers connected to the Internet
- Documents are prepared using HyperText Markup Language (HTML)
- A browser application program is used to access the web
- The browser displays HTML documents that include *links* to other documents
- Each link references a *Uniform Resource Locator* (URL) that gives the name of the machine and the location of the given document
- Let's see what happens when a user clicks on a link

Source: Communication Networks, Leon-Garcia and Widjaja

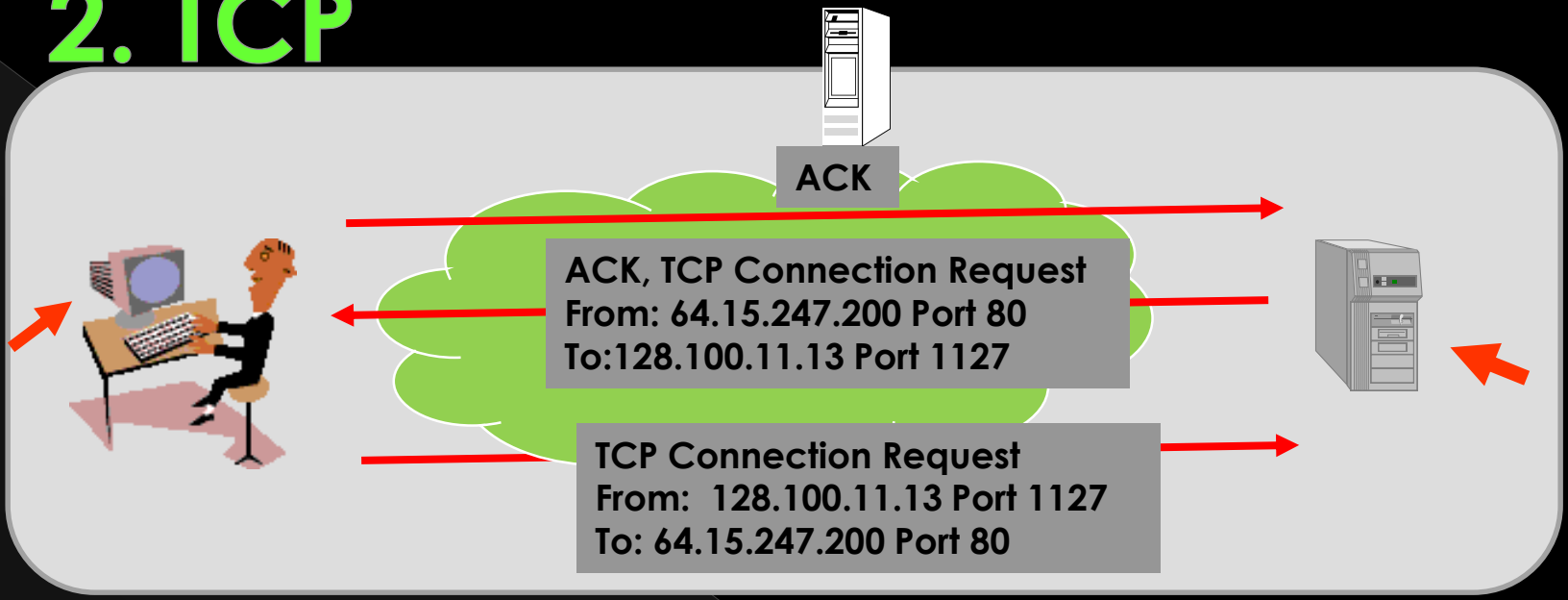
1. DNS



- User clicks on http://www.nytimes.com/
- URL contains Internet name of machine (www.nytimes.com), but not Internet address
- Internet needs Internet address to send information to a machine
- Browser software uses Domain Name System (DNS) protocol to send query for Internet address
- DNS system responds with Internet address

Source: Communication Networks, Leon-Garcia and Widjaja

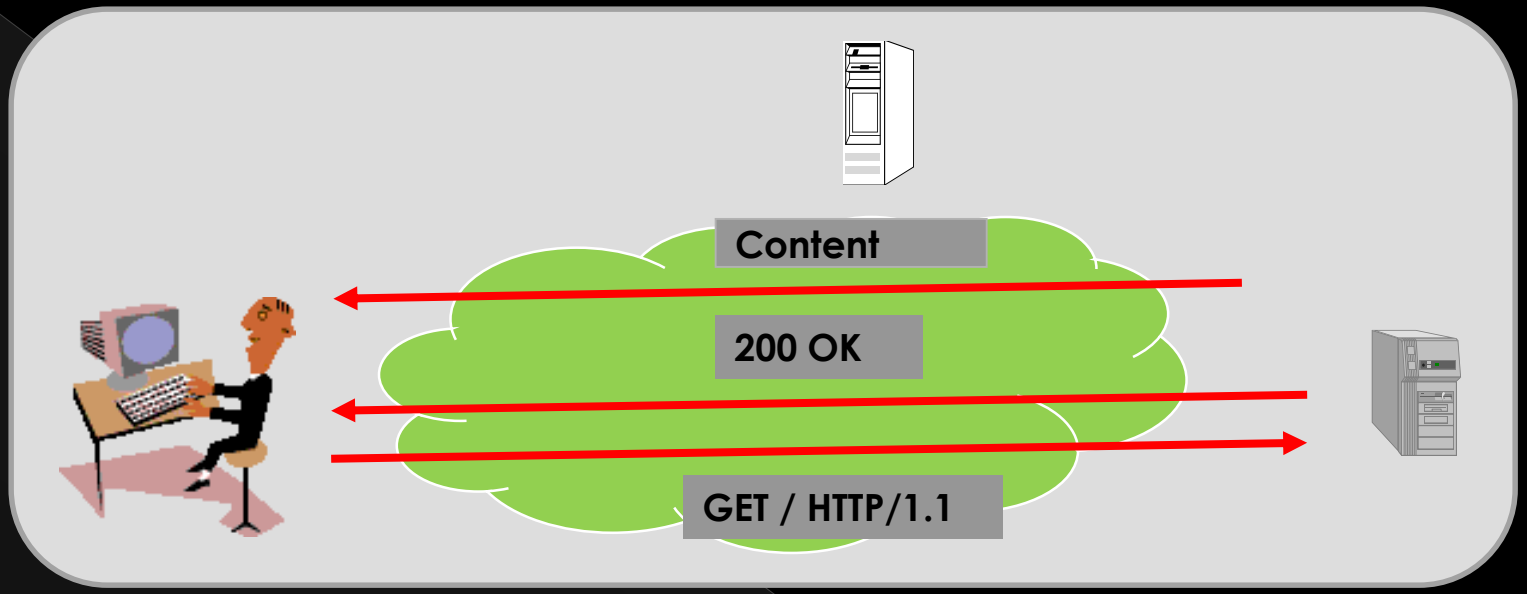
2. TCP



- Browser software uses HyperText Transfer Protocol (HTTP) to send request for document
- HTTP server waits for requests by listening to a well-known port number (80 for HTTP)
- HTTP client sends request messages through an "ephemeral port number," e.g. 1127
- HTTP needs a Transmission Control Protocol (TCP) connection between the HTTP client and the HTTP server to transfer messages reliably

Source: Communication Networks, Leon-Garcia and Widjaja

3. HTTP



- HTTP client sends its request message: "GET …"
- HTTP server sends a status response: "200 OK"
- HTTP server sends requested file
- Browser displays document
- Clicking a link sets off a chain of events across the Internet!
- Let's see how protocols & layers come into play…

Source: Communication Networks, Leon-Garcia and Widjaja

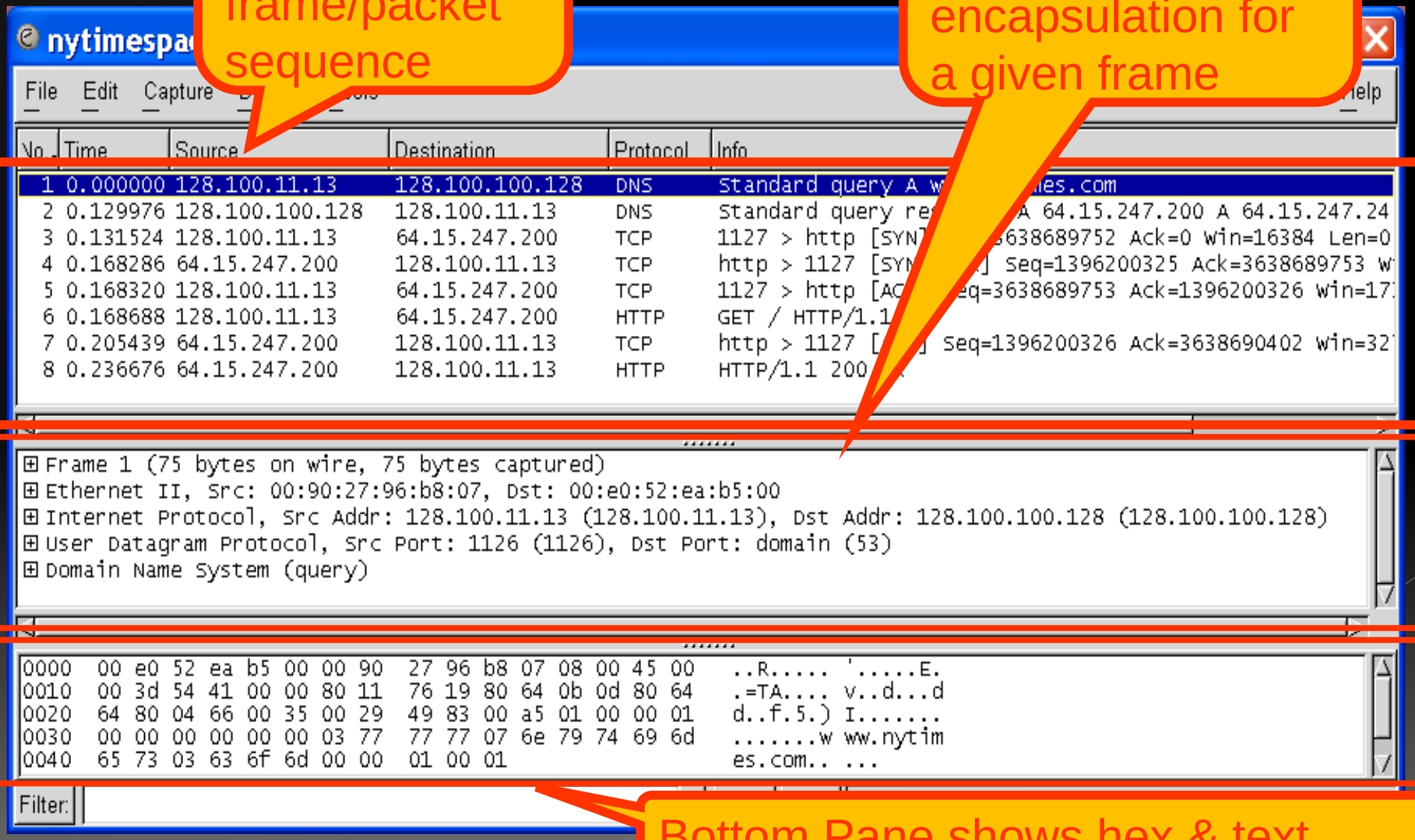
How the layers work together: Network Analyzer Example

- User clicks on http://www.nytimes.com/
- *Wireshark* (*Ethereal*) network analyzer captures all frames observed by its Ethernet NIC
- Sequence of frames and contents of frame can be examined in detail down to individual bytes

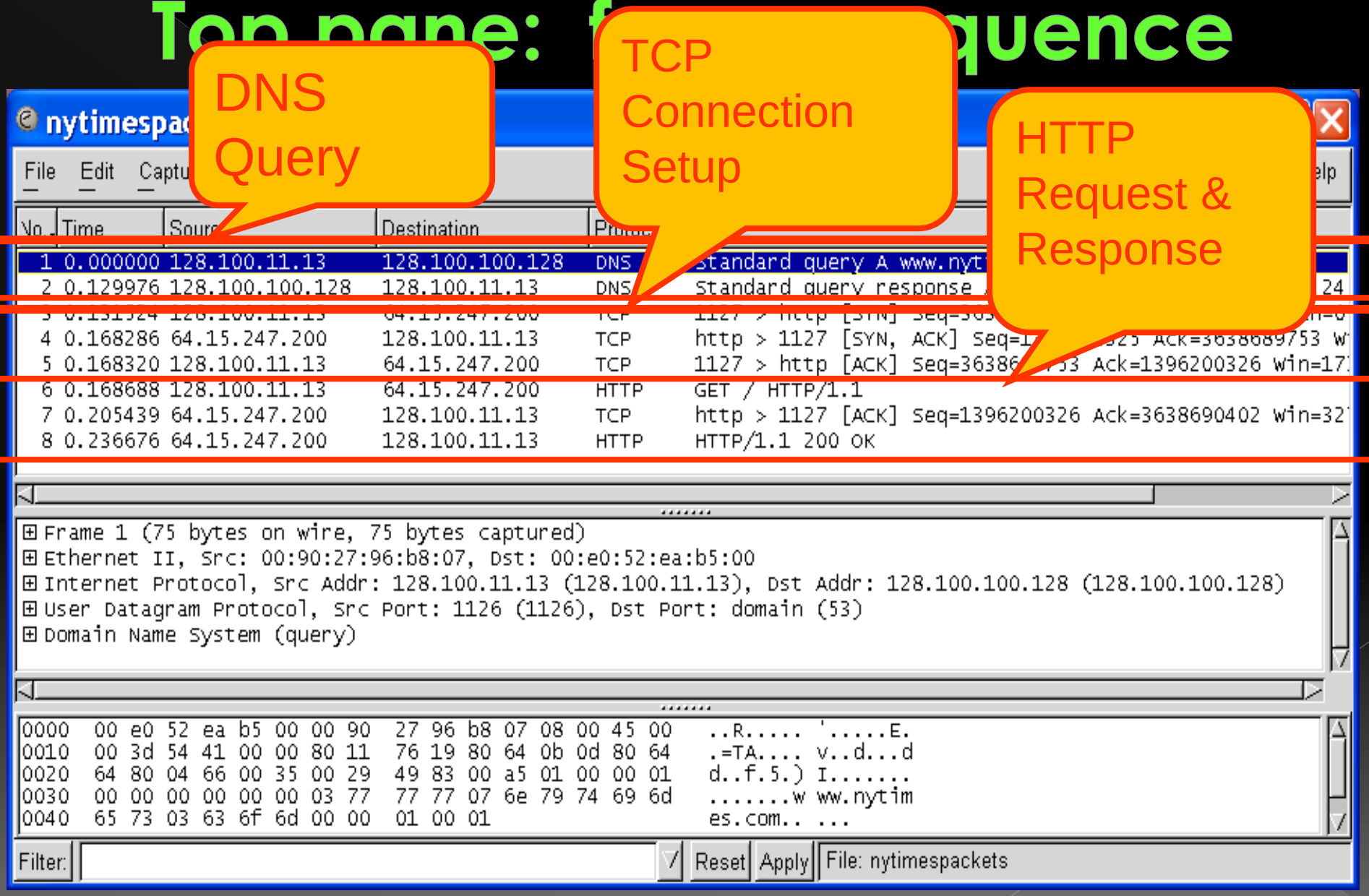
ACTIVITY FOUR:
Grabbing Cookies and Passwords with Wireshark

- Wireshark
  - http://www.wireshark.org/download.html
- Grabbing cookies and password
  - http://www.html-kit.com/tools/cookietester/

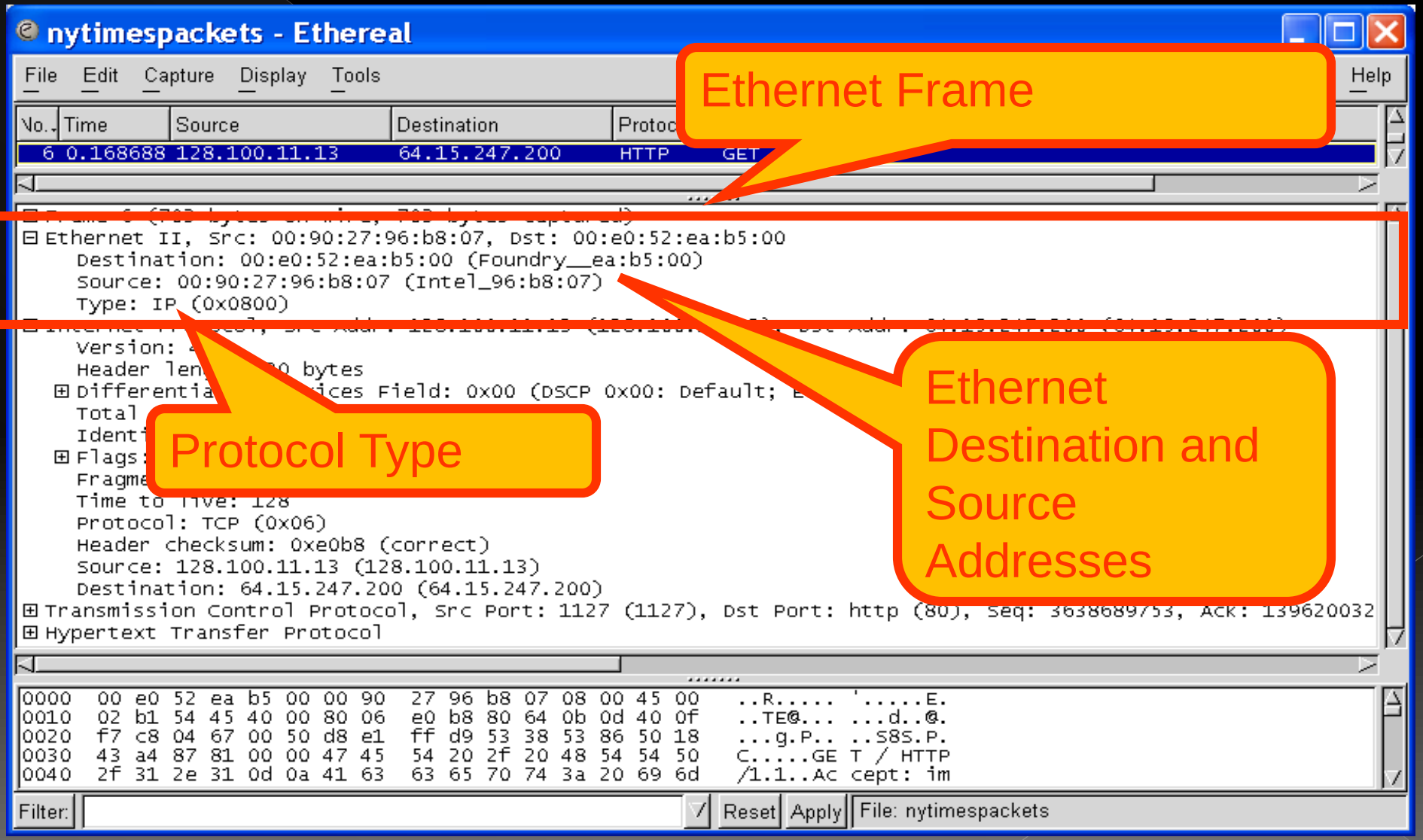
E indows


Top Pane shows frame/packet sequence
Middle Pane shows encapsulation for a given frame
nytimespa
File Edit Capture
Help
No. Time Source Destination Protocol Info
1 0.000000 128.100.11.13 128.100.100.128 DNS Standard query A w es.com
2 0.129976 128.100.100.128 128.100.11.13 DNS Standard query re A 64.15.247.200 A 64.15.247.24
3 0.131524 128.100.11.13 64.15.247.200 TCP 1127 > http [SYN 638689752 Ack=0 Win=16384 Len=0
4 0.168286 64.15.247.200 128.100.11.13 TCP http > 1127 [SYN] Seq=1396200325 Ack=3638689753 W
5 0.168320 128.100.11.13 64.15.247.200 TCP 1127 > http [AC eq=3638689753 Ack=1396200326 Win=17
6 0.168688 128.100.11.13 64.15.247.200 HTTP GET / HTTP/1.1
7 0.205439 64.15.247.200 128.100.11.13 TCP http > 1127 [ ] Seq=1396200326 Ack=3638690402 Win=32
8 0.236676 64.15.247.200 128.100.11.13 HTTP HTTP/1.1 200
⊞ Frame 1 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: 00:90:27:96:b8:07, Dst: 00:e0:52:ea:b5:00
⊞ Internet Protocol, Src Addr: 128.100.11.13 (128.100.11.13), Dst Addr: 128.100.100.128 (128.100.100.128)
⊞ User Datagram Protocol, Src Port: 1126 (1126), Dst Port: domain (53)
⊞ Domain Name System (query)
0000 00 e0 52 ea b5 00 00 90 27 96 b8 07 08 00 45 00 ..R..... '.....E.
0010 00 3d 54 41 00 00 80 11 76 19 80 64 0b 0d 80 64 .=TA.... v..d...d
0020 64 80 04 66 00 35 00 29 49 83 00 a5 01 00 00 01 d..f.5.) I.......
0030 00 00 00 00 00 00 03 77 77 77 07 6e 79 74 69 6d ....w ww.nytim
0040 65 73 03 63 6f 6d 00 00 01 00 01 es.com.. ...
Filter:
Bottom Pane shows hex & text

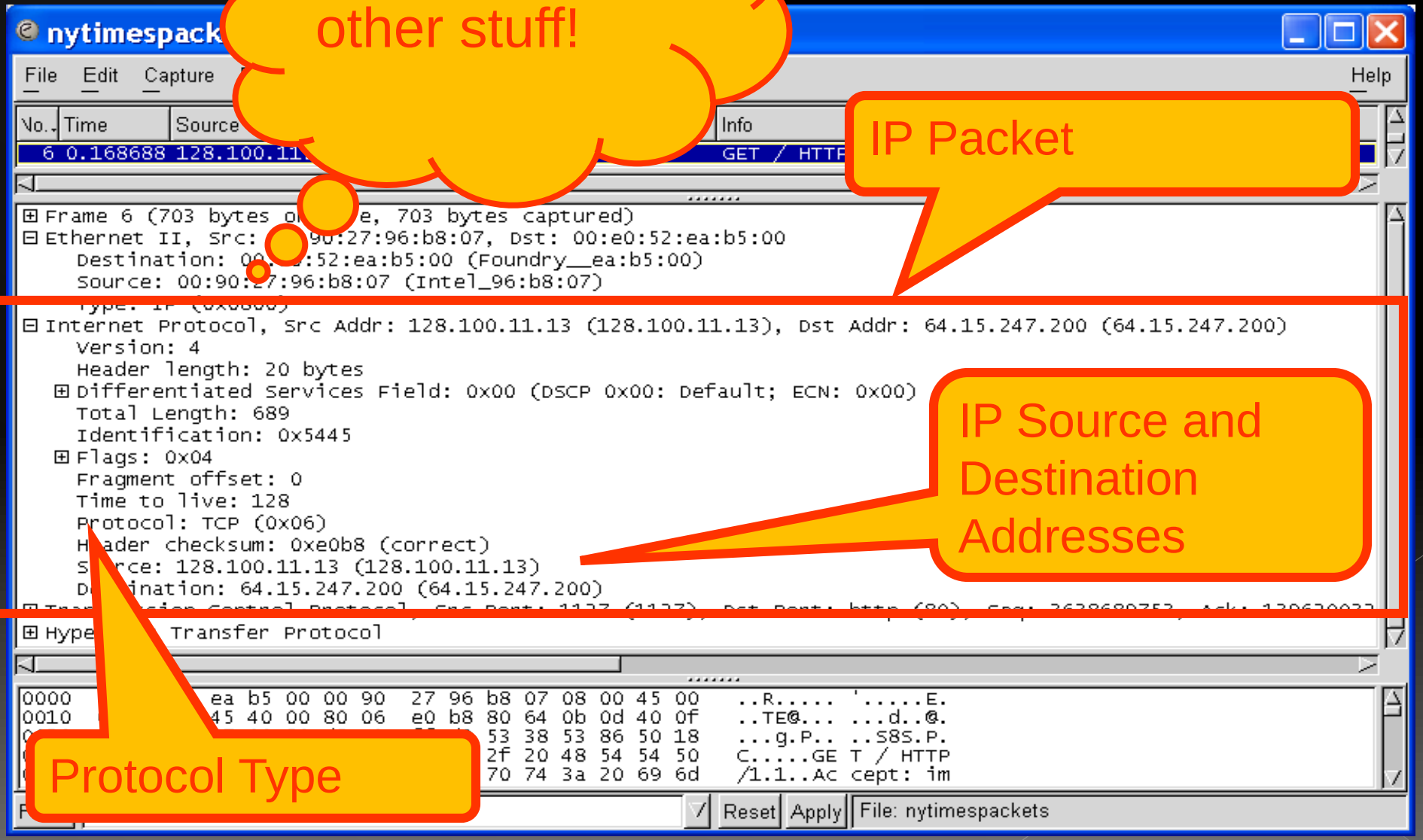
Top pane: f quence



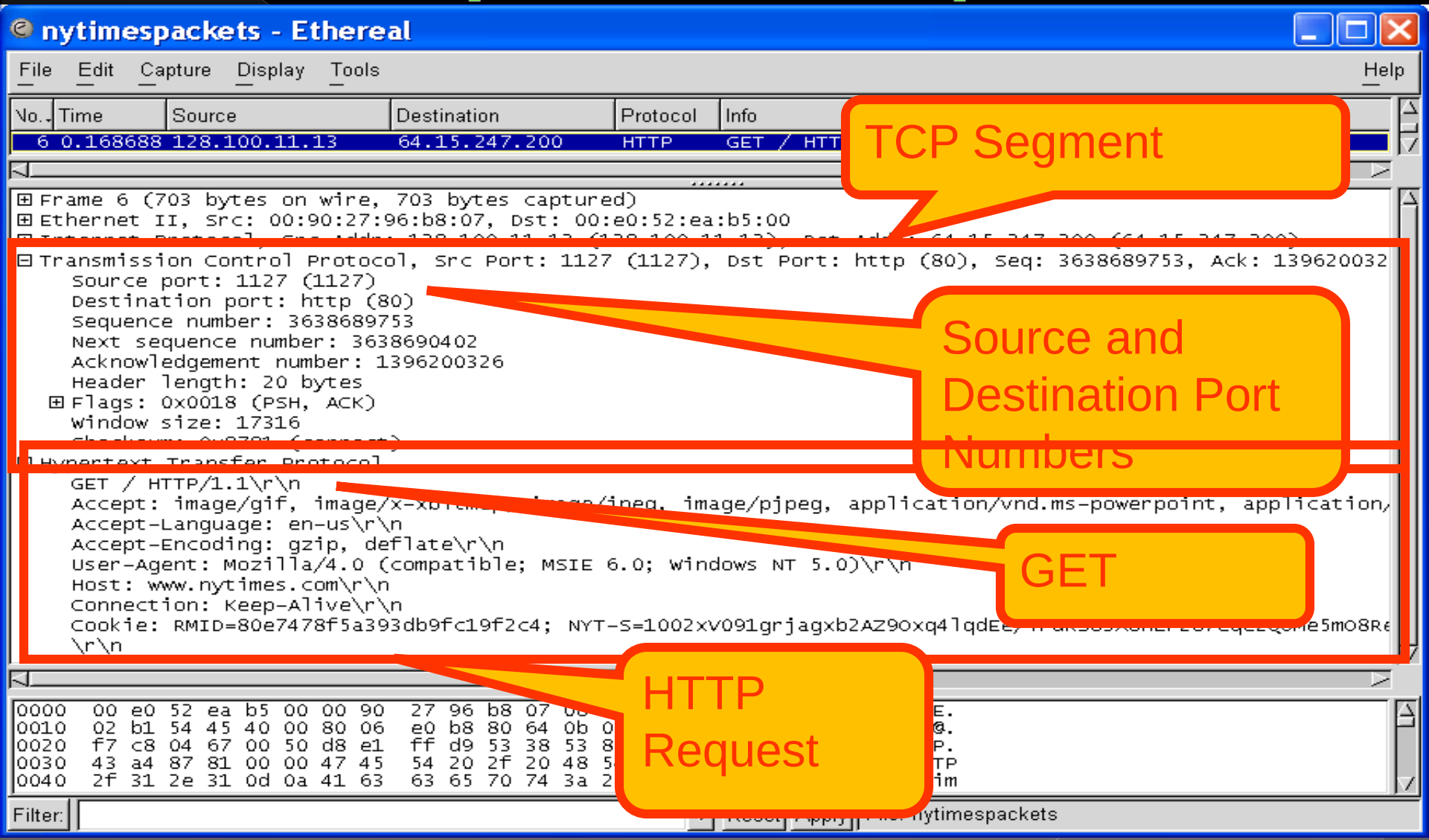
Middle pane: Encapsulation



Mid Encapsulation

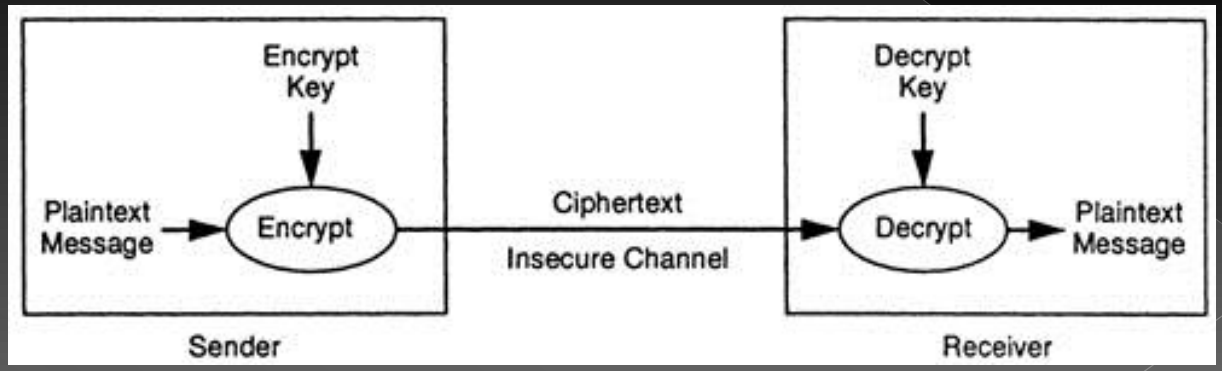


Middle pane: Encapsulation



Encryption Terms

- Plaintext – Original Message
- Algorithm – Transformation Procedure
- Key – Variable used to scramble message
- Ciphertext – Resulting garbled output



Source: class note by Rob Guess

ACTIVITY FIVE:
Encryption and Decryption

- PKI Demo
  - http://infoencrypt.com/

Steganography (1)

- The Science of Hiding Information
  - History – Tablets, shaved heads
  - Now - Images, sounds, other files
- Data is frequently encrypted
  - Frequency analysis can detect this

Source: class note by Rob Guess

Steganography (2)

The image in which we want to hide another image:
'Arctic hare' – Copyright photos courtesy of Robert E. Barber, Barber Nature Photography (REBarber@msn.com)

Source: http://petitcolas.net/fabien/steganography/image_downgrading/index.html

Steganography (3)

The image we wish to hide: ‘F15’ – Copyright photo courtesy of Toni Lankerd, 18347 Woodland Ridge Dr. Apt #7, Spring Lake, MI 49456, U.S.A. (tlankerd@wmis.net)

Source: http://petitcolas.net/fabien/steganography/image_downgrading/index.html

ACTIVITY SIX:
Steganography

- Download Steganography software
  - http://www.openstego.com/
  - http://www.secretcodebreaker.com/steganography.html
- Sample Execution

ACTIVITY SEVEN:
Digital Photo Scavenger Hunt

- http://regex.info/exif.cgi
  - First, make sure you have location based services enabled on the students phones. Then they can take their phones and snap pictures around landmarks on your campus. Afterwards, they could connect their phones and transfer the image, or email them to themselves. Then all they have to do is upload the images to the address above. The images with EXIF data will then plot on a Google Map.

DAY FOUR

Activity Eight:
Prepare the Friday presentation

- Prepare the presentation, including
  - Systematic Approach of Digital Investigation
  - How to use
    - Digital Photo Scavenger Hunt
    - Wireshark
    - FTK
    - Steganography

Activity Nine:
Field Trip (Tabletop Activity)

- 10:00-10:30: Transportation to City Government Building
- 10:30-10:45: Introduction
- 10:45-11:30: Tabletop Part I
- 11:30-12:15: Lunch
- 12:15-3:15: Field Exercise
- 3:15-4:00: Tabletop Part II
- 4:00-4:30: Guest Speaker
- 4:30: Wrap-up and back to campus

DAY FIVE

Activity Ten:
Prepare the Friday presentation

- Prepare the presentation, including
  - Systematic Approach of Digital Investigation
  - How to use
    - Digital Photo Scavenger Hunt
    - Wireshark
    - FTK
    - Steganography

Any Questions?