CYBERSECURITY TRAINING: Bridging the Gap from Policy to Practice

Mari Galloway
Lisa Jiggetts
Marcelle Lee

December 6, 2017

“Tell me and I forget. Teach me and I remember. Involve me and I learn.”

~ Benjamin Franklin

About Mari

- Vulnerability Engineer, Las Vegas Sands Corp
- 9+ years in IT and Cybersecurity
- Certifications - CISSP, GIAC (various), CEH to name a few
- Hobbies: Arts & Crafts, Baking, geeking out!

About Lisa

- Founder/CEO Women’s Society of Cyberjutsu
- 18+ years in cyber, Military vet
- Tech and gadget lover
- Hobbies: soccer, painting, eating

About Marcelle

- Threat Researcher, LookingGlass Cyber Solutions, Inc.
- Co-founder and CEO, Fractal Security Group, LLC
- Cybersecurity trainer - academia and contract
- Compulsive volunteer - WSC, ISACA, ISSA, NIST
- Certifications - CSX-P, GCIA, GPEN, CISSP, to name a few
- Cyber competition enthusiast

About Women’s Society of Cyberjutsu

- 501c(3) nonprofit passionate about helping and empowering women to succeed in the cybersecurity field.
- Cybersecurity community-organization
- Offer workshops/classes/study groups, networking events, conference group attendance, job board, volunteer opps
- Cyberjutsu Girls Academy - Girls in STEM program for MS girls

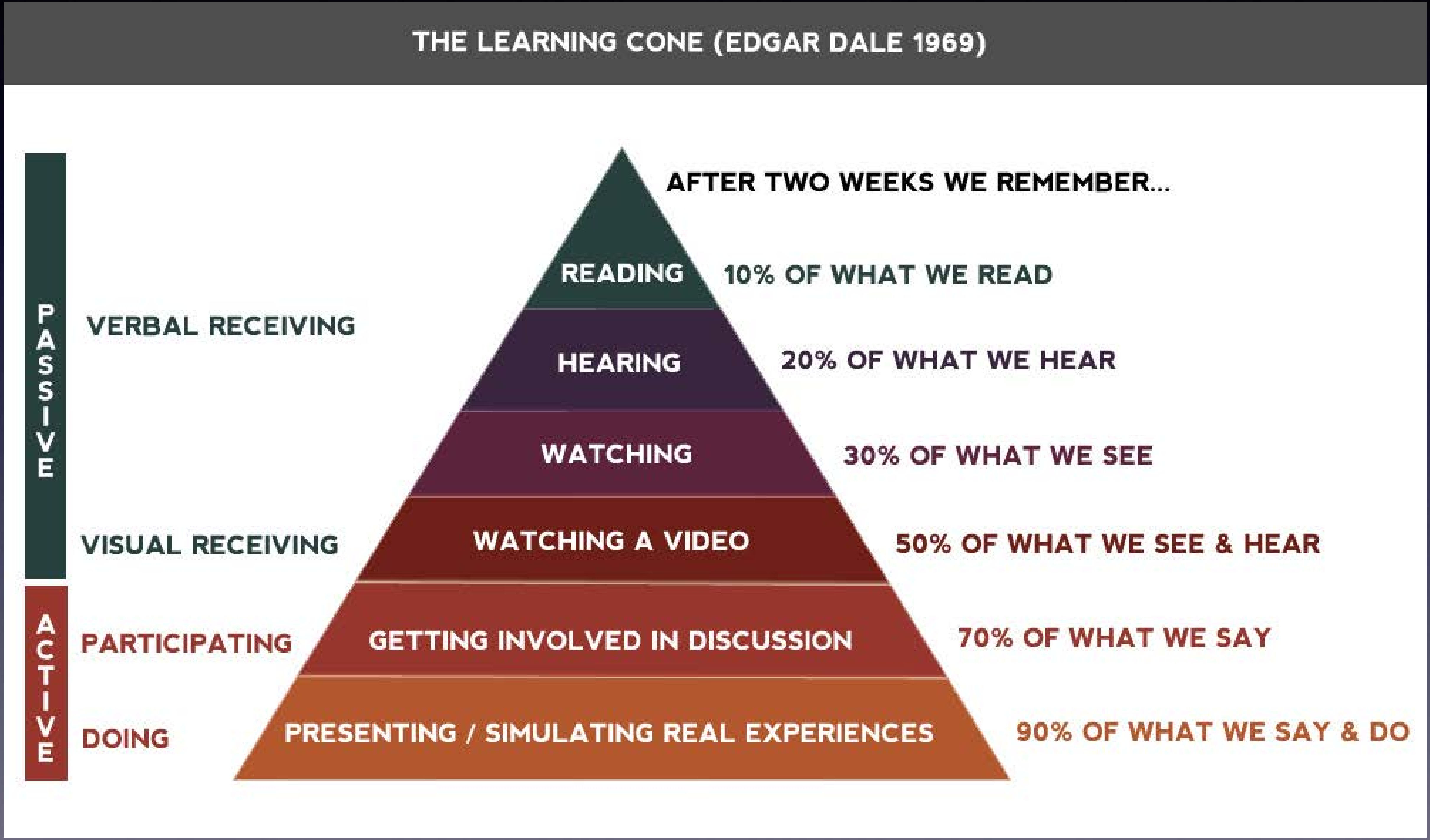
Training Topics

- Cybersecurity Basics
- Network Security
- Command Line Fu
- Digital Forensics
- Penetration Testing
- Python Programming
- Building a Home Lab Environment
- Certification Prep

Curriculum Development

- Experiential learning or “hands-on-keys”
- Emphasis on critical thinking
- Encourage questioning and exploration
- Real world examples and applications
- Don’t be a “sage on the stage”

Dale Cone of Learning



THE LEARNING CONE (EDGAR DALE 1969)

AFTER TWO WEEKS WE REMEMBER...

PASSIVE

VERBAL RECEIVING

READING — 10% OF WHAT WE READ

HEARING — 20% OF WHAT WE HEAR

WATCHING — 30% OF WHAT WE SEE

VISUAL RECEIVING

WATCHING A VIDEO — 50% OF WHAT WE SEE & HEAR

ACTIVE

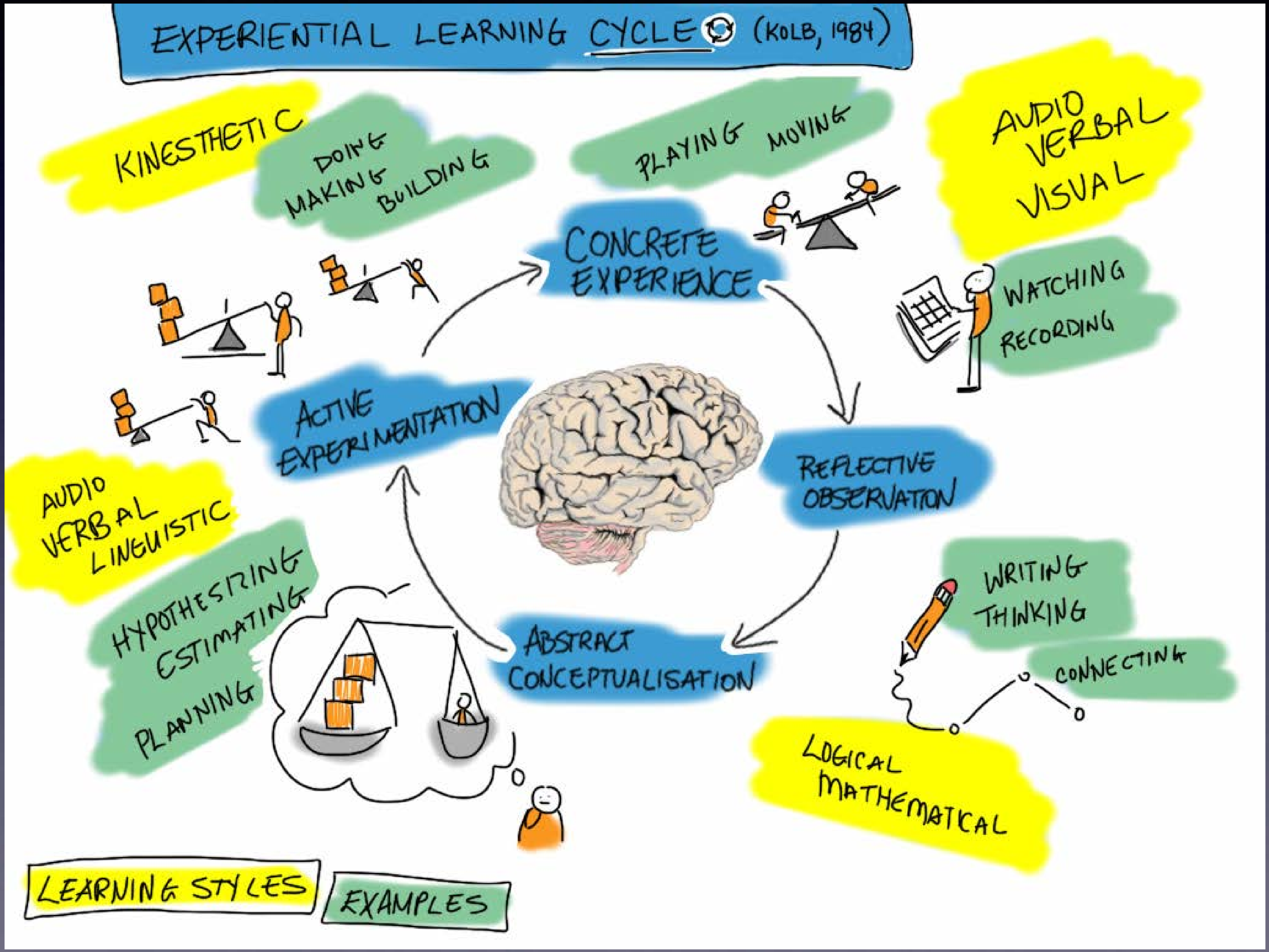
PARTICIPATING

GETTING INVOLVED IN DISCUSSION — 70% OF WHAT WE SAY

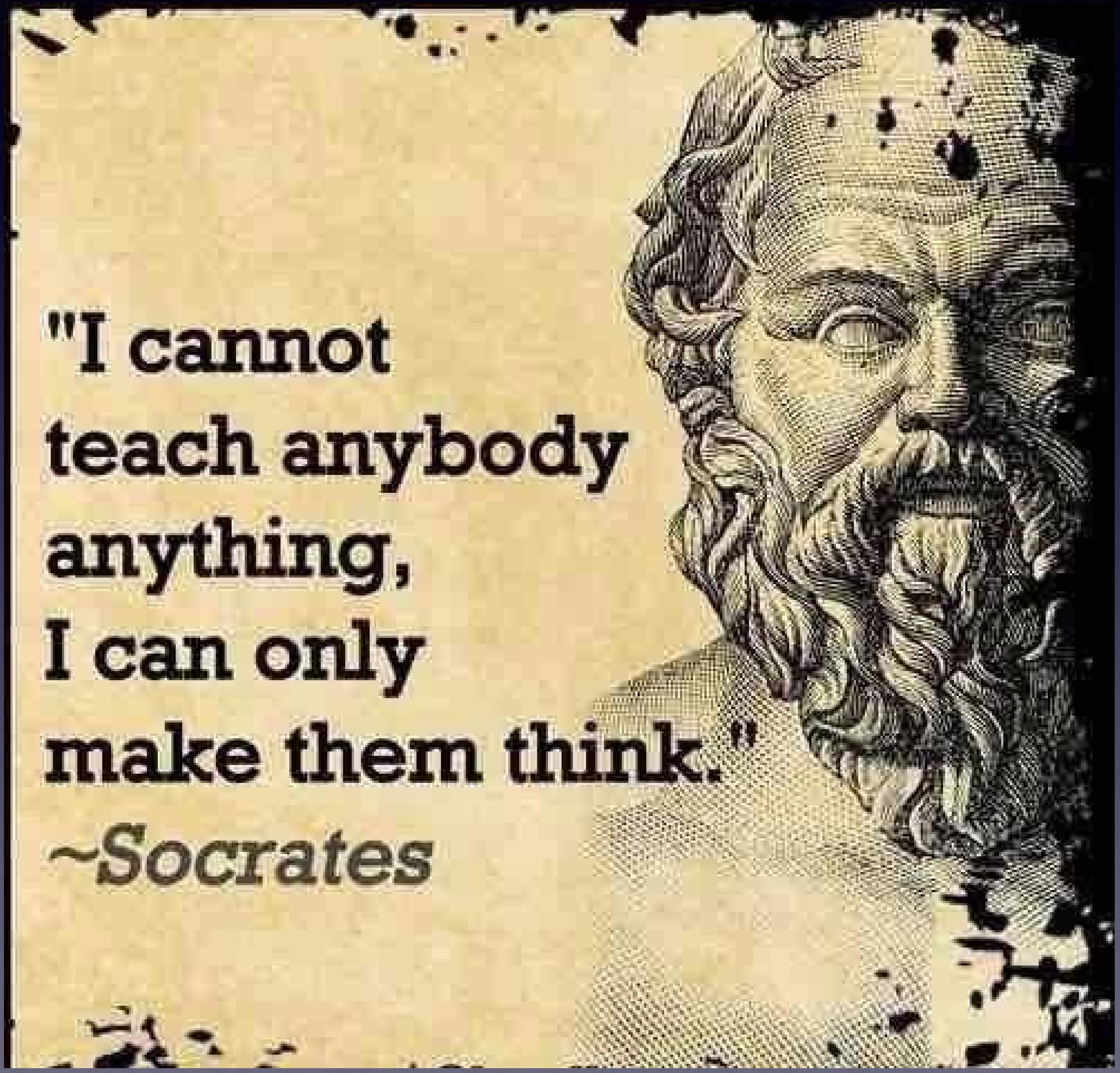
DOING

PRESENTING / SIMULATING REAL EXPERIENCES — 90% OF WHAT WE SAY & DO

Kolb Experiential Learning Cycle



Socratic Method



"I cannot
teach anybody
anything,
I can only
make them think."
~Socrates

Participant Experience Levels

100 < 2 years sec exp. / some IT

200 < 4 years sec exp.

300 > 4 years sec exp.

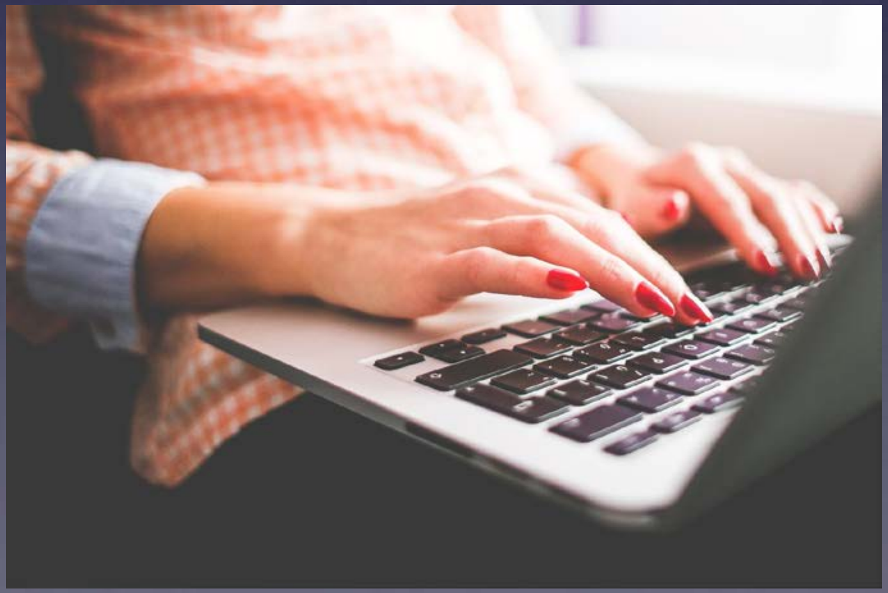
Level 100 courses are designed for students with little to no previous IT Security experience, or no experience in the topic(s) being covered. These courses are meant to be introductory level, or provide the training for entry level certifications.

Level 200 courses are designed for students with some security experience, looking to advance or learn in new topics.

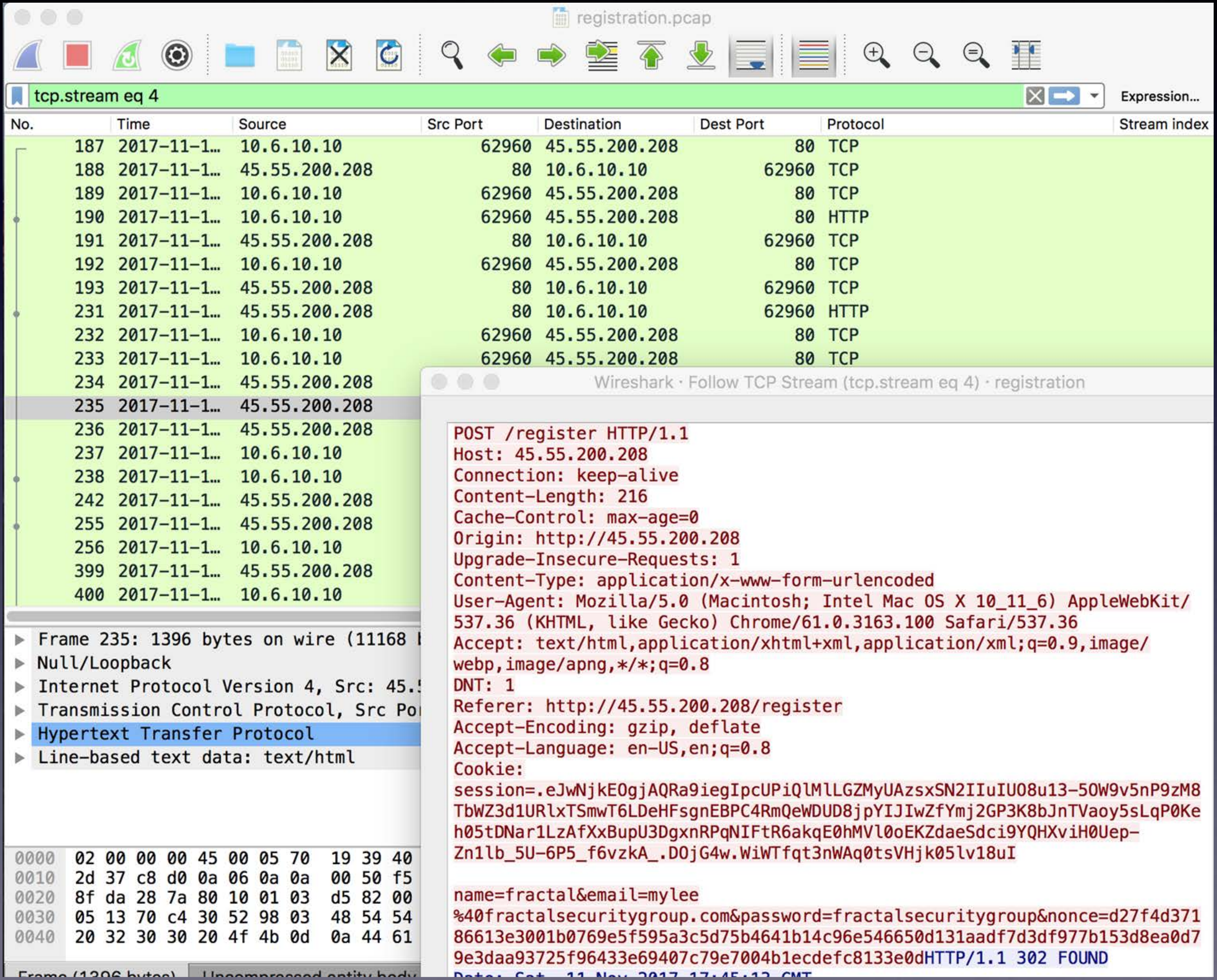
Level 300 courses are designed to offer expert level courses and training on specific topics. Typically, a general understanding and knowledge of the topic being presented is an expected prerequisite.

Hands-on-Keys

- Workshops
- Study Groups
- Competition Practice



Example: Hands-on-Keys



```
tcp.stream eq 4
```

```
No.       Time           Source          Src Port  Destination     Dest Port  Protocol    Stream index
    187  2017-11-1…  10.6.10.10          62960  45.55.200.208         80  TCP
    188  2017-11-1…  45.55.200.208          80  10.6.10.10         62960  TCP
    189  2017-11-1…  10.6.10.10          62960  45.55.200.208         80  TCP
    190  2017-11-1…  10.6.10.10          62960  45.55.200.208         80  HTTP
    191  2017-11-1…  45.55.200.208          80  10.6.10.10         62960  TCP
    192  2017-11-1…  10.6.10.10          62960  45.55.200.208         80  TCP
    193  2017-11-1…  45.55.200.208          80  10.6.10.10         62960  TCP
    231  2017-11-1…  45.55.200.208          80  10.6.10.10         62960  HTTP
    232  2017-11-1…  10.6.10.10          62960  45.55.200.208         80  TCP
    233  2017-11-1…  10.6.10.10          62960  45.55.200.208         80  TCP
    234  2017-11-1…  45.55.200.208
    235  2017-11-1…  45.55.200.208
    236  2017-11-1…  45.55.200.208
    237  2017-11-1…  10.6.10.10
    238  2017-11-1…  10.6.10.10
    242  2017-11-1…  45.55.200.208
    255  2017-11-1…  45.55.200.208
    256  2017-11-1…  10.6.10.10
    399  2017-11-1…  45.55.200.208
    400  2017-11-1…  10.6.10.10
```

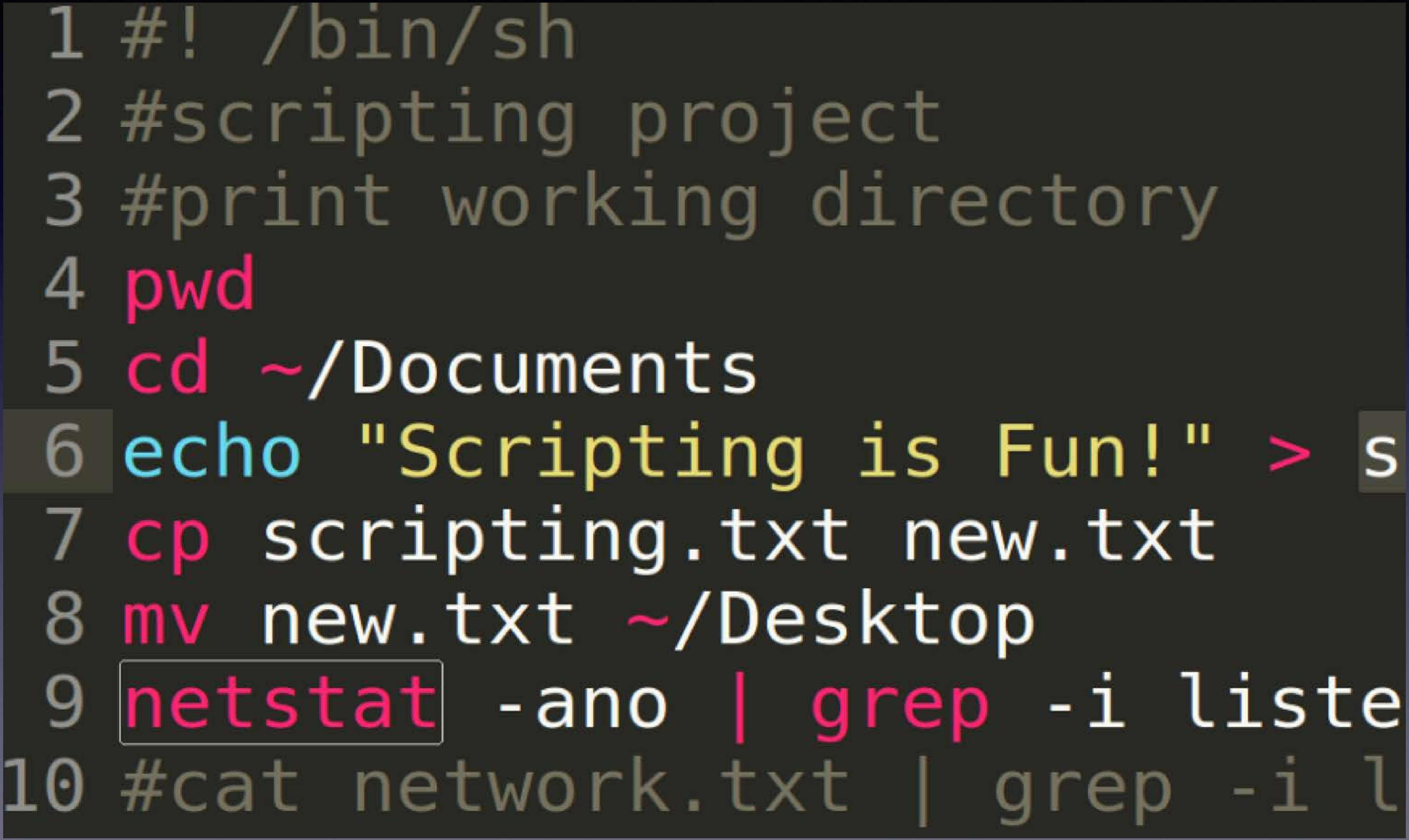
```
▶ Frame 235: 1396 bytes on wire (11168 b
▶ Null/Loopback
▶ Internet Protocol Version 4, Src: 45.5
▶ Transmission Control Protocol, Src Po
▶ Hypertext Transfer Protocol
▶ Line-based text data: text/html
```

```
0000  02 00 00 00 45 00 05 70  19 39 40
0010  2d 37 c8 d0 0a 06 0a 0a  00 50 f5
0020  8f da 28 7a 80 10 01 03  d5 82 00
0030  05 13 70 c4 30 52 98 03  48 54 54
0040  20 32 30 30 20 4f 4b 0d  0a 44 61
```

Wireshark · Follow TCP Stream (tcp.stream eq 4) · registration

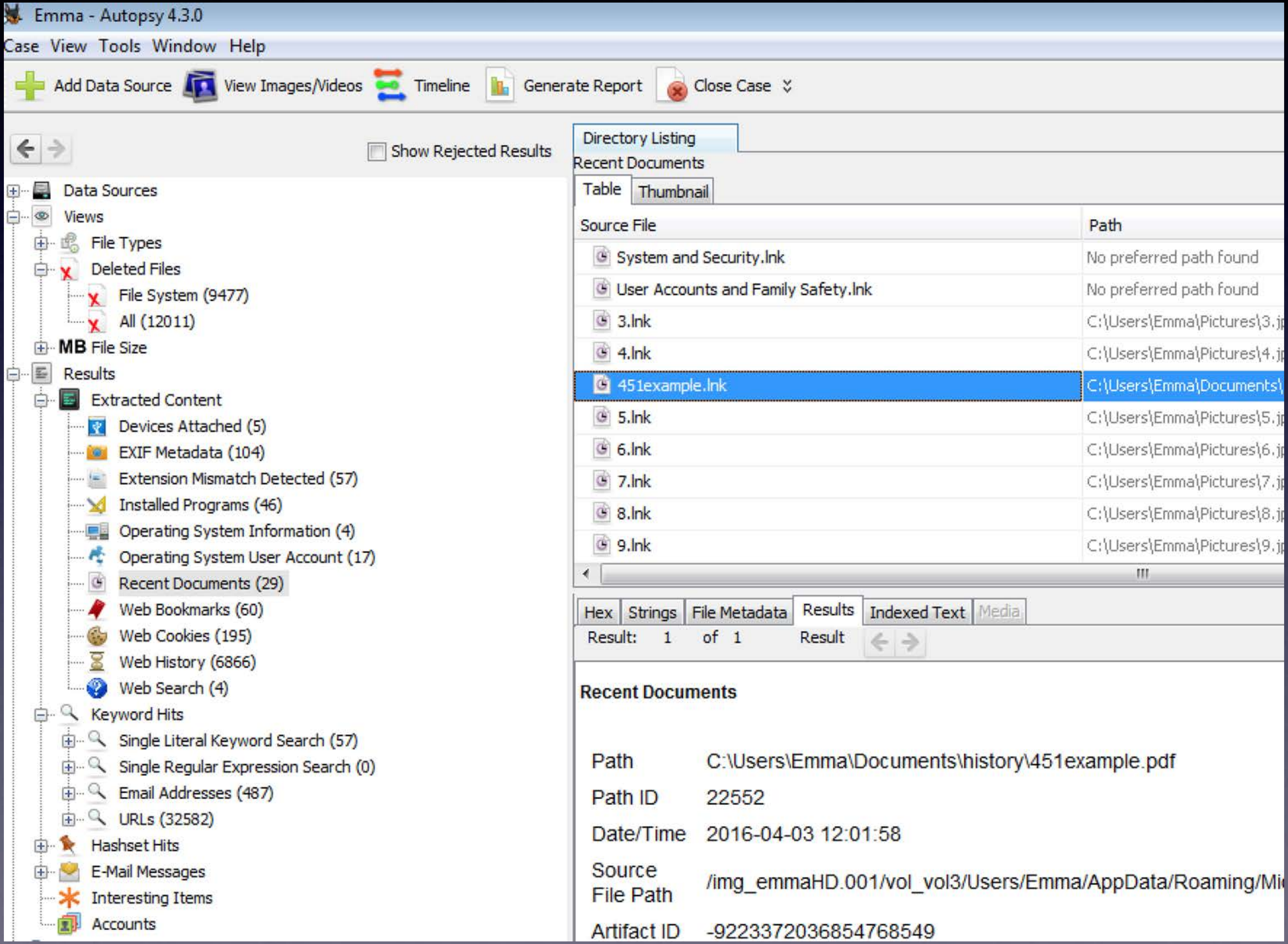
```
POST /register HTTP/1.1
Host: 45.55.200.208
Connection: keep-alive
Content-Length: 216
Cache-Control: max-age=0
Origin: http://45.55.200.208
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8
DNT: 1
Referer: http://45.55.200.208/register
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie:
session=.eJwNjkEOgjAQRa9iegIpcUPiQlMlLGZMyUAzsxSN2IIuIUO8u13-5OW9v5nP9zM8
TbWZ3d1URlxTSmwT6LDeHFsgnEBPC4RmQeWDUD8jpYIJIwZfYmj2GP3K8bJnTVaoy5sLqP0Ke
h05tDNar1LzAfXxBupU3DgxnRPqNIFtR6akqE0hMVl0oEKZdaeSdci9YQHXviH0Uep-
Zn1lb_5U-6P5_f6vzkA_.DOjG4w.WiWTfqt3nWAq0tsVHjk05lv18uI

name=fractal&email=mylee
%40fractalsecuritygroup.com&password=fractalsecuritygroup&nonce=d27f4d371
86613e3001b0769e5f595a3c5d75b4641b14c96e546650d131aadf7d3df977b153d8ea0d7
9e3daa93725f96433e69407c79e7004b1ecdefc8133e0dHTTP/1.1 302 FOUND
Date: Sat, 11 Nov 2017 17:45:13 GMT
```

Example: Hands-on-Keys



```
#! /bin/sh
#scripting project
#print working directory
pwd
cd ~/Documents
echo "Scripting is Fun!" > s
cp scripting.txt new.txt
mv new.txt ~/Desktop
netstat -ano | grep -i liste
#cat network.txt | grep -i l
```

Example: Hands-on-Keys

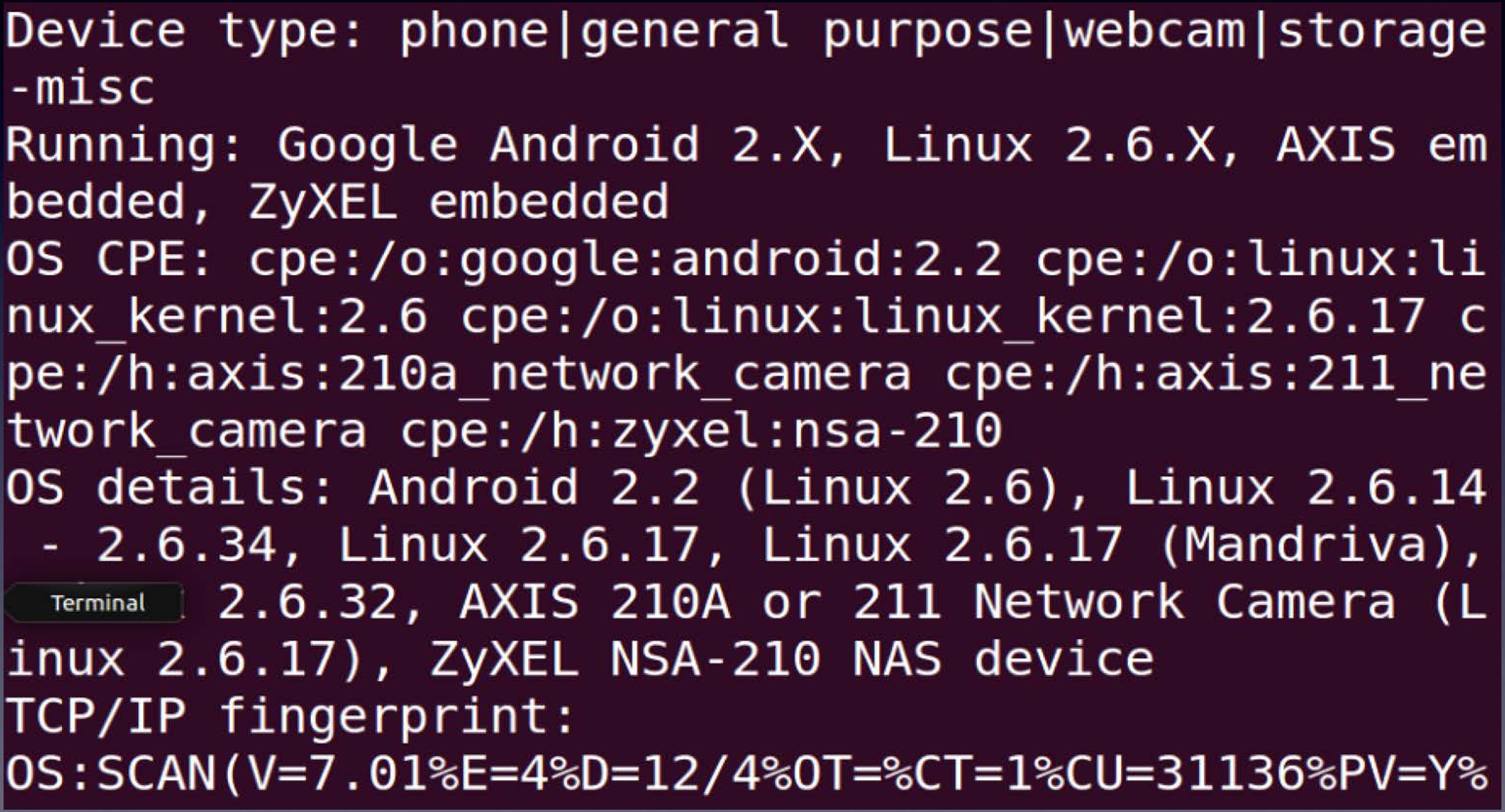


Source File	Path
System and Security.lnk	No preferred path found
User Accounts and Family Safety.lnk	No preferred path found
3.lnk	C:\Users\Emma\Pictures\3.j
4.lnk	C:\Users\Emma\Pictures\4.j
451example.lnk	C:\Users\Emma\Documents\
5.lnk	C:\Users\Emma\Pictures\5.j
6.lnk	C:\Users\Emma\Pictures\6.j
7.lnk	C:\Users\Emma\Pictures\7.j
8.lnk	C:\Users\Emma\Pictures\8.j
9.lnk	C:\Users\Emma\Pictures\9.j

Recent Documents

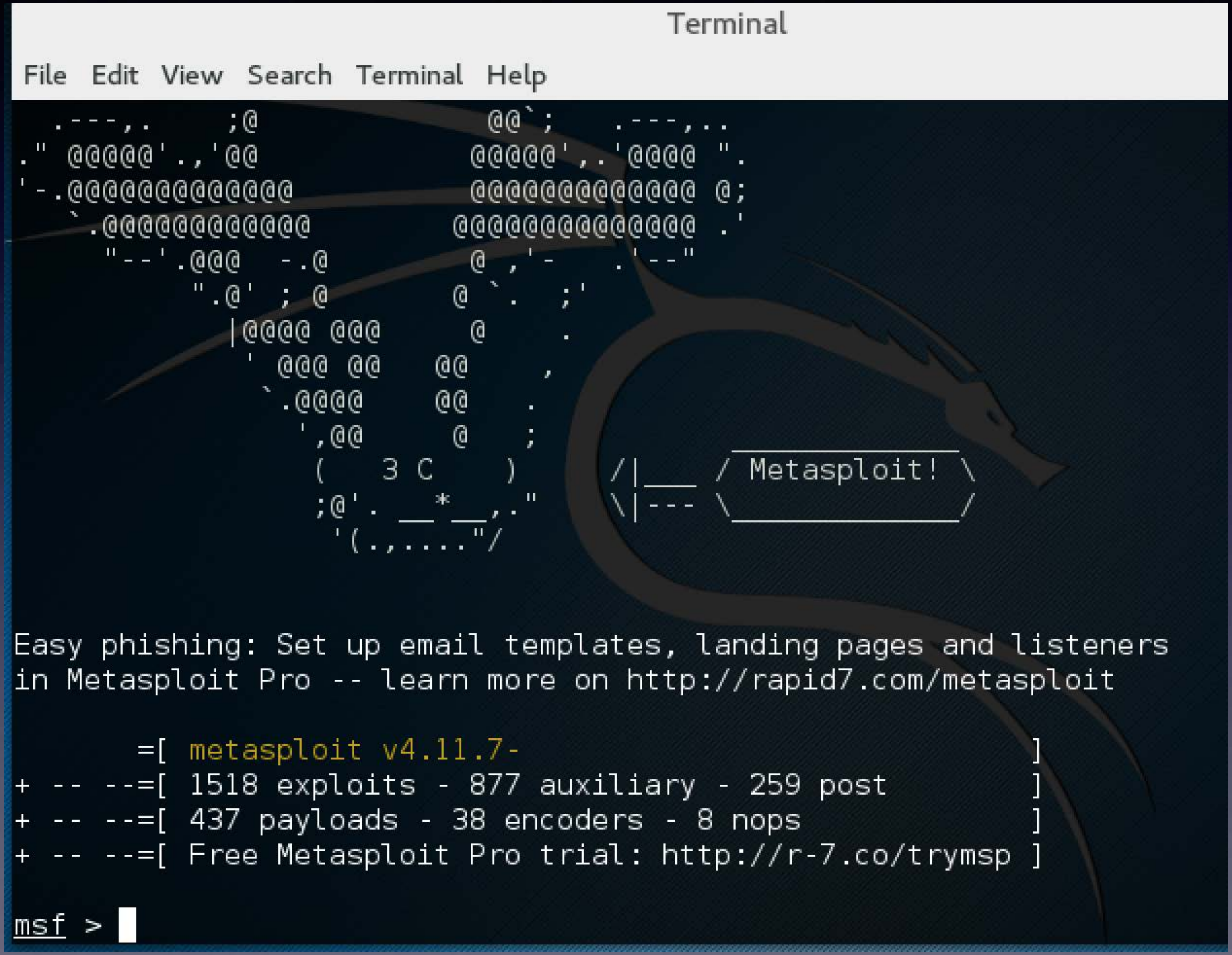
Path	C:\Users\Emma\Documents\history\451example.pdf
Path ID	22552
Date/Time	2016-04-03 12:01:58
Source File Path	/img_emmaHD.001/vol_vol3/Users/Emma/AppData/Roaming/Mi
Artifact ID	-9223372036854768549

Example: Hands-on-Keys



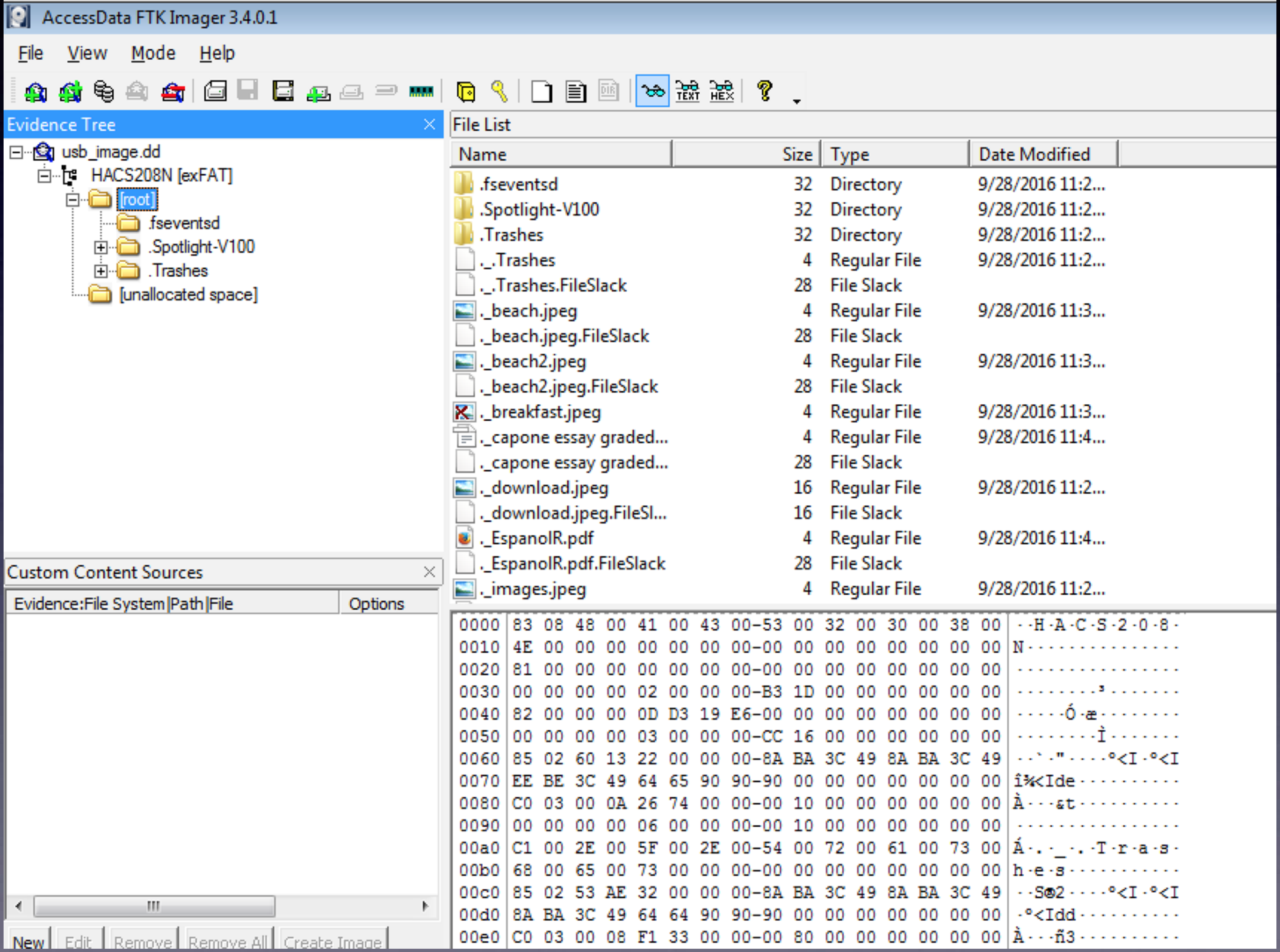
```
Device type: phone|general purpose|webcam|storage
-misc
Running: Google Android 2.X, Linux 2.6.X, AXIS em
bedded, ZyXEL embedded
OS CPE: cpe:/o:google:android:2.2 cpe:/o:linux:li
nux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.17 c
pe:/h:axis:210a_network_camera cpe:/h:axis:211_ne
twork_camera cpe:/h:zyxel:nsa-210
OS details: Android 2.2 (Linux 2.6), Linux 2.6.14
 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriva),
[illegible] 2.6.32, AXIS 210A or 211 Network Camera (L
inux 2.6.17), ZyXEL NSA-210 NAS device
TCP/IP fingerprint:
OS:SCAN(V=7.01%E=4%D=12/4%OT=%CT=1%CU=31136%PV=Y%
```

Example: Hands-on-Keys



```
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                 (   3 C    )     /|___ / Metasploit! \
                 ;@'. __*__,."    \|--- \_____________/
                  '(.,...."/


Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.7-                             ]
+ -- --=[ 1518 exploits - 877 auxiliary - 259 post        ]
+ -- --=[ 437 payloads - 38 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

Example: Hands-on-Keys



```
usb_image.dd
  HACS208N [exFAT]
    [root]
      .fseventsd
      .Spotlight-V100
      .Trashes
    [unallocated space]
```

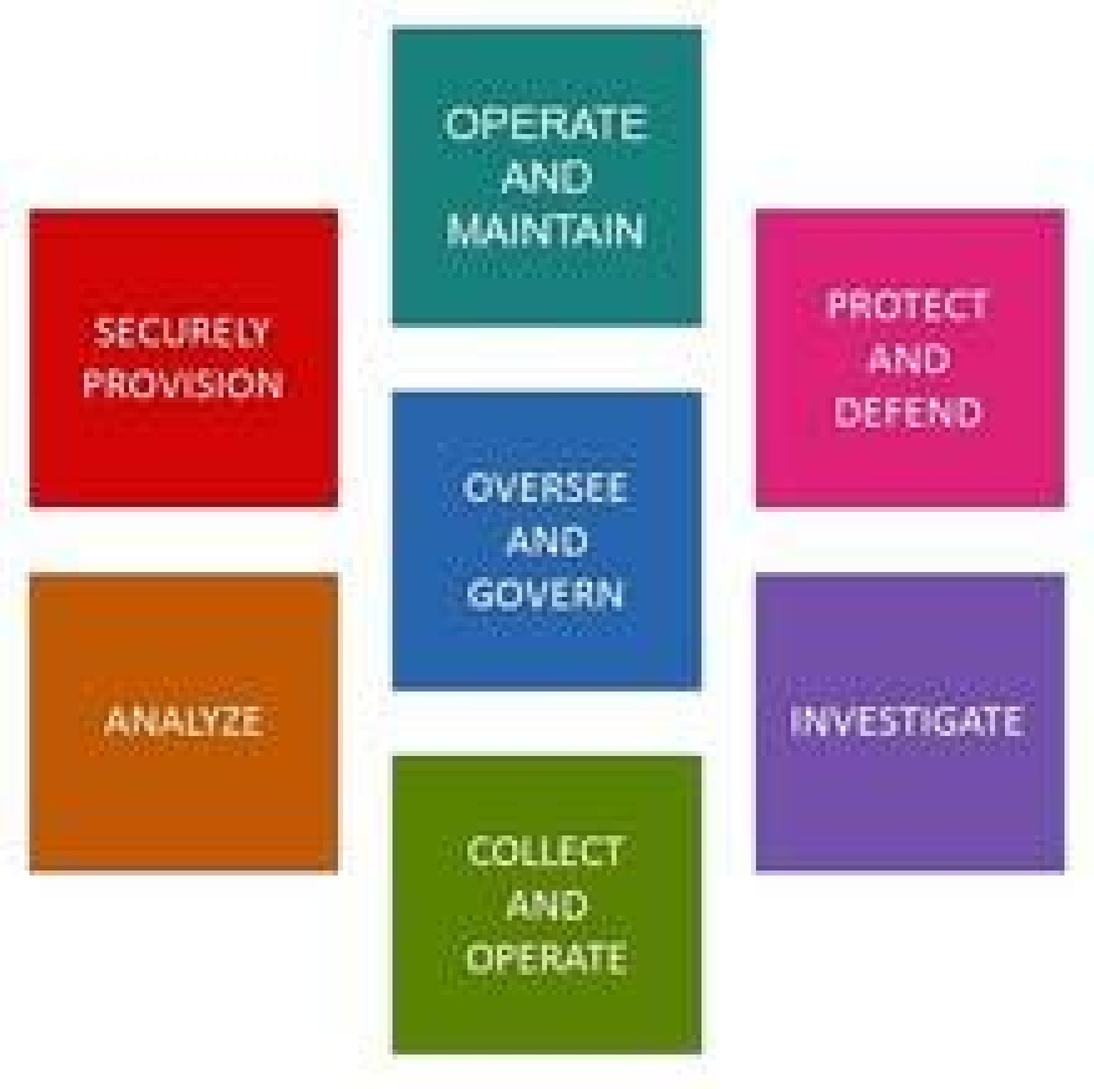
Name	Size	Type	Date Modified
.fseventsd	32	Directory	9/28/2016 11:2...
.Spotlight-V100	32	Directory	9/28/2016 11:2...
.Trashes	32	Directory	9/28/2016 11:2...
._.Trashes	4	Regular File	9/28/2016 11:2...
._.Trashes.FileSlack	28	File Slack	
._beach.jpeg	4	Regular File	9/28/2016 11:3...
._beach.jpeg.FileSlack	28	File Slack	
._beach2.jpeg	4	Regular File	9/28/2016 11:3...
._beach2.jpeg.FileSlack	28	File Slack	
._breakfast.jpeg	4	Regular File	9/28/2016 11:3...
._capone essay graded...	4	Regular File	9/28/2016 11:4...
._capone essay graded...	28	File Slack	
._download.jpeg	16	Regular File	9/28/2016 11:2...
._download.jpeg.FileSl...	16	File Slack	
._EspanolR.pdf	4	Regular File	9/28/2016 11:4...
._EspanolR.pdf.FileSlack	28	File Slack	
._images.jpeg	4	Regular File	9/28/2016 11:2...

```
0000 83 08 48 00 41 00 43 00-53 00 32 00 30 00 38 00  ··H·A·C·S·2·0·8·
0010 4E 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  N···············
0020 81 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
0030 00 00 00 00 02 00 00 00-B3 1D 00 00 00 00 00 00  ········³·······
0040 82 00 00 00 0D D3 19 E6-00 00 00 00 00 00 00 00  ·····Ó·æ········
0050 00 00 00 00 03 00 00 00-CC 16 00 00 00 00 00 00  ········Ì·······
0060 85 02 60 13 22 00 00 00-8A BA 3C 49 8A BA 3C 49  ··`·"····°<I·°<I
0070 EE BE 3C 49 64 65 90 90-90 00 00 00 00 00 00 00  î¾<Ide··········
0080 C0 03 00 0A 26 74 00 00-00 10 00 00 00 00 00 00  À···&t··········
0090 00 00 00 00 06 00 00 00-00 10 00 00 00 00 00 00  ················
00a0 C1 00 2E 00 5F 00 2E 00-54 00 72 00 61 00 73 00  Á·.·_·.·T·r·a·s·
00b0 68 00 65 00 73 00 00 00-00 00 00 00 00 00 00 00  h·e·s···········
00c0 85 02 53 AE 32 00 00 00-8A BA 3C 49 8A BA 3C 49  ··S®2····°<I·°<I
00d0 8A BA 3C 49 64 64 90 90-90 00 00 00 00 00 00 00  ·°<Idd··········
00e0 C0 03 00 08 F1 33 00 00-00 80 00 00 00 00 00 00  À···ñ3··········
```

Remote Participation

- Attend from home
- LMS - Canvas, Moodle, etc.
- Connect - Webex, JoinMe, etc.
- Features live chat w/ instructor and/or assistant
- Recorded for later viewing

Cybersecurity Workforce Framework



NIST Special Publication 800-181

Questions?

info@womenscyberjutsu.org
mari.galloway@womenscyberjutsu.org
mlee@lookingglasscyber.com

Resources: https://goo.gl/iUr4H7