SELF-PROTECTIVE BEHAVIORS OVER PUBLIC WIFI NETWORKS

David Maimon, Michael Becker

Department of Criminology and Criminal Justice

University of Maryland

Sushant Patil

Information Science School

University of Maryland

Jonathan Katz

Computer Science Department

University of Maryland

This project is funded by the National Science Foundation award # 1444633 and #1223634

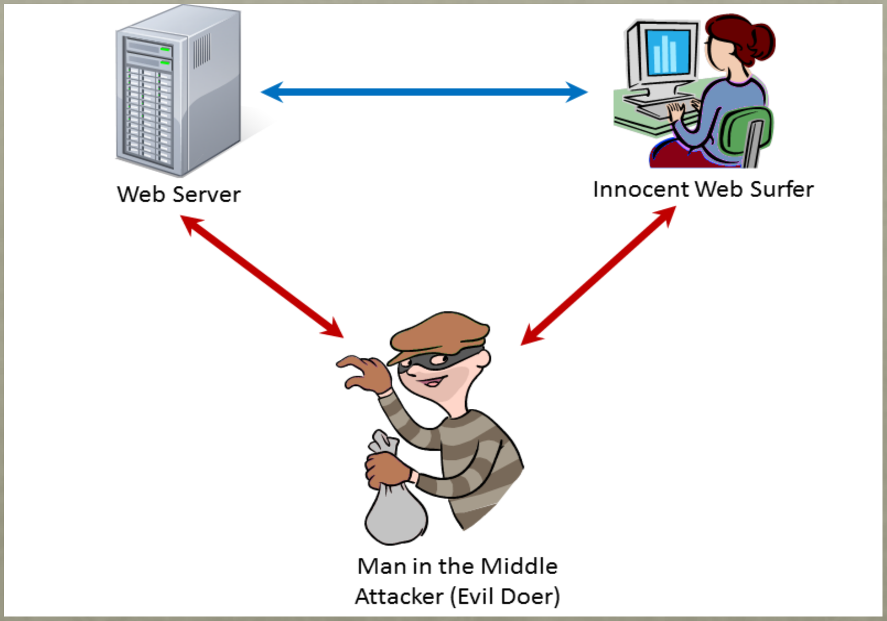
PROJECT GOALS

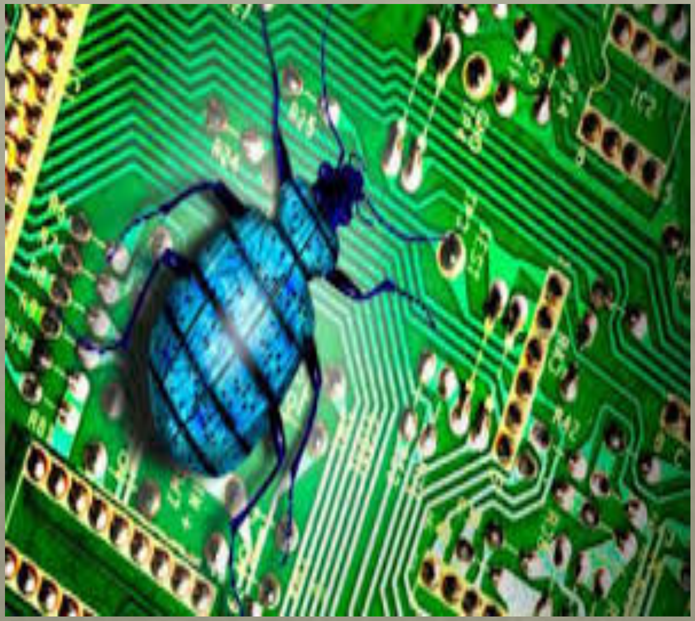
- Identify the most common risky online behaviors that public WIFI users are involved in over the network

- Explore whether uncertainty regarding the owner of a WiFi network shape users' avoidance from accessing websites that handle sensitive information

PUBLIC WIFI

- Public WIFI networks allow users to log in to the Internet from various public locations and at all times of day.
- Risks:





VICTIMS' SELF PROTECTIVE BEHAVIORS

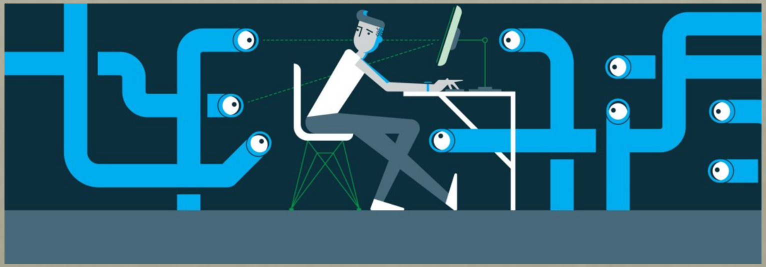
- Different types of self protective behaviors and their effectiveness in preventing violent crime (Guerette & Santenna 2010; Block and Skogen 1984)

Forceful Resistance

Non Forceful Resistance

Self Protective Behaviors in Cyber Space

- Apply security solutions



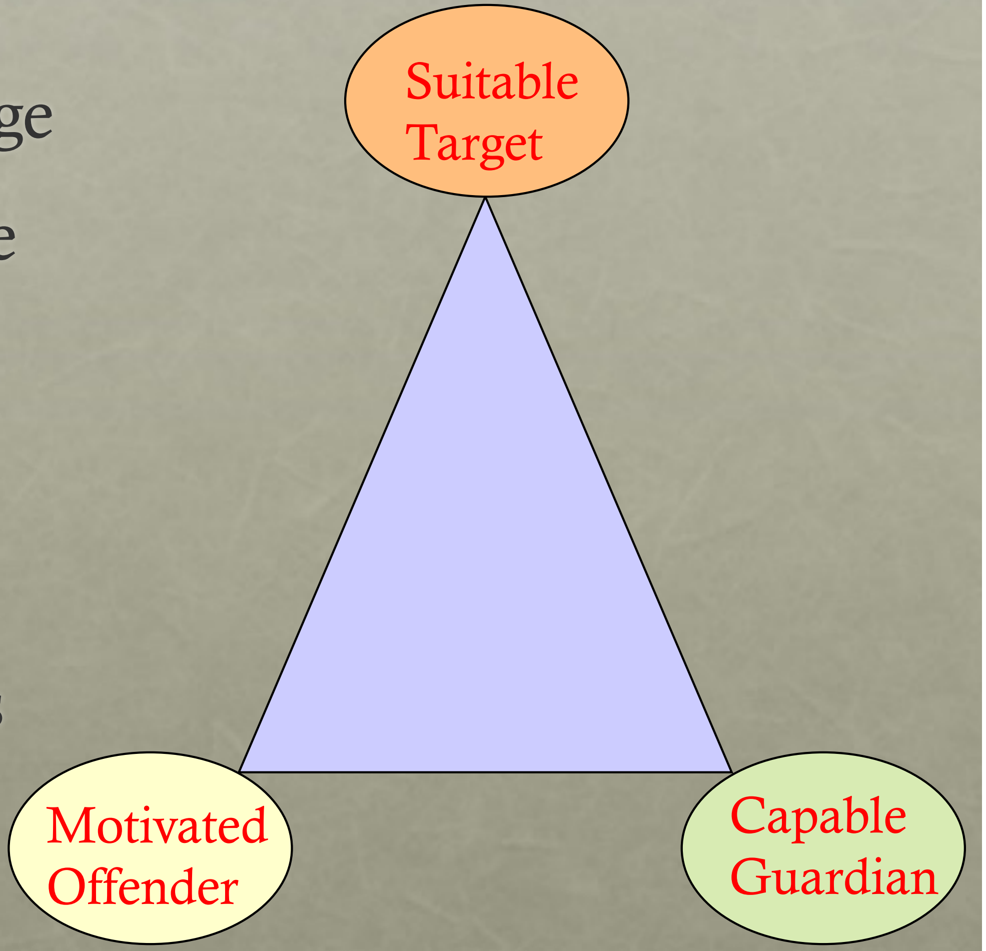
- Protect privacy
- Online vigilance

- Avoid accessing and providing sensitive information

ROUTINE ACTIVITY THEORY

- Three elements must converge in time and space for a crime to occur:

1. Motivated offender
2. Suitable target
3. Lack of capable guardians



Theoretical Implications

- As the level of victim resistance increases, the effort for the offender will also increase, and in turn, will reduce the probability of crime completion (Clarke 1997)

© U. Baumgarten via Getty Images

Situational Crime Prevention Strategies

- Both property and violent offenses may be effectively prevented by reducing the opportunity for criminal events and deterring offenders from violating the law.

    - *Increase offenders' effort*
    - *Increase offenders' risks*
    - *Reduce offenders' rewards*
    - *Reduce provocations*
    - *Remove excuse*

THEORETICAL IMPLICATIONS

- As the level of victim resistance increases, the effort for the offender will also increase, and in turn, will reduce the probability of crime completion (Clarke 1997)

- Victim engagement in non-forceful resistance will reduce offenders' emotional arousal and will have low odds of initiation and completion of a criminal event (Cornish and Clarke 2003)

© U. Baumgarten via Getty Images

RESEARCH QUESTION 1

- How common avoidance from accessing websites that handle sensitive information (banking, email, social networks and personal cloud) among WiFi networks is?

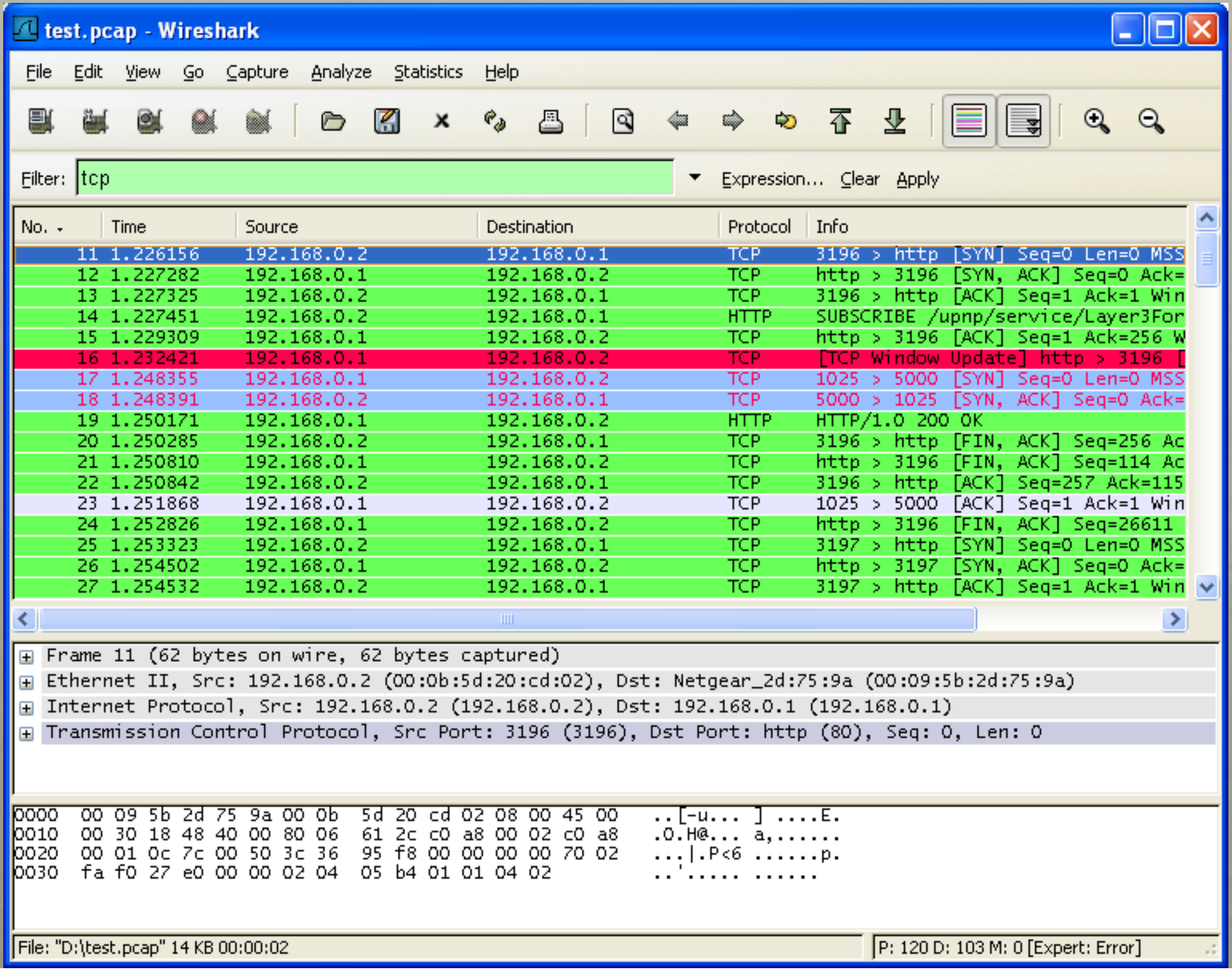
RESEARCH QUESTION 2

- Does uncertainty regarding the owner of a WiFi network shape users' avoidance from accessing websites that handle sensitive information ?

RESEARCH DESIGN- PHASE 1

- 24 public WIFI locations in the state of MD and DC
  - 16 Coffee houses
  - 7 Restaurants
  - 1 Hotel lobby

PUBLIC WIFI DATA



Filter: tcp

```
No. .   Time       Source        Destination   Protocol  Info
   11 1.226156    192.168.0.2   192.168.0.1   TCP       3196 > http [SYN] Seq=0 Len=0 MSS
   12 1.227282    192.168.0.1   192.168.0.2   TCP       http > 3196 [SYN, ACK] Seq=0 Ack=
   13 1.227325    192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=1 Ack=1 Win
   14 1.227451    192.168.0.2   192.168.0.1   HTTP      SUBSCRIBE /upnp/service/Layer3For
   15 1.229309    192.168.0.1   192.168.0.2   TCP       http > 3196 [ACK] Seq=1 Ack=256 W
   16 1.232421    192.168.0.1   192.168.0.2   TCP       [TCP Window Update] http > 3196 [
   17 1.248355    192.168.0.1   192.168.0.2   TCP       1025 > 5000 [SYN] Seq=0 Len=0 MSS
   18 1.248391    192.168.0.2   192.168.0.1   TCP       5000 > 1025 [SYN, ACK] Seq=0 Ack=
   19 1.250171    192.168.0.1   192.168.0.2   HTTP      HTTP/1.0 200 OK
   20 1.250285    192.168.0.2   192.168.0.1   TCP       3196 > http [FIN, ACK] Seq=256 Ac
   21 1.250810    192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=114 Ac
   22 1.250842    192.168.0.2   192.168.0.1   TCP       3196 > http [ACK] Seq=257 Ack=115
   23 1.251868    192.168.0.1   192.168.0.2   TCP       1025 > 5000 [ACK] Seq=1 Ack=1 Win
   24 1.252826    192.168.0.1   192.168.0.2   TCP       http > 3196 [FIN, ACK] Seq=26611
   25 1.253323    192.168.0.2   192.168.0.1   TCP       3197 > http [SYN] Seq=0 Len=0 MSS
   26 1.254502    192.168.0.1   192.168.0.2   TCP       http > 3197 [SYN, ACK] Seq=0 Ack=
   27 1.254532    192.168.0.2   192.168.0.1   TCP       3197 > http [ACK] Seq=1 Ack=1 Win
```

```
⊞ Frame 11 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)
⊞ Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)
⊞ Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0
```

```
0000  00 09 5b 2d 75 9a 00 0b  5d 20 cd 02 08 00 45 00   ..[-u... ] ....E.
0010  00 30 18 48 40 00 80 06  61 2c c0 a8 00 02 c0 a8   .0.H@... a,......
0020  00 01 0c 7c 00 50 3c 36  95 f8 00 00 00 00 70 02   ...|.P<6 ......p.
0030  fa f0 27 e0 00 00 02 04  05 b4 01 01 04 02         ..'..... ......
```

File: "D:\test.pcap" 14 KB 00:00:02 | P: 120 D: 103 M: 0 [Expert: Error]

Date: 02/23/2015, Monday

IP Address: 192.168.1.108

Uplink: 3.34 Mbps Downlink: 11.02 Mbps

No. of Males: 27

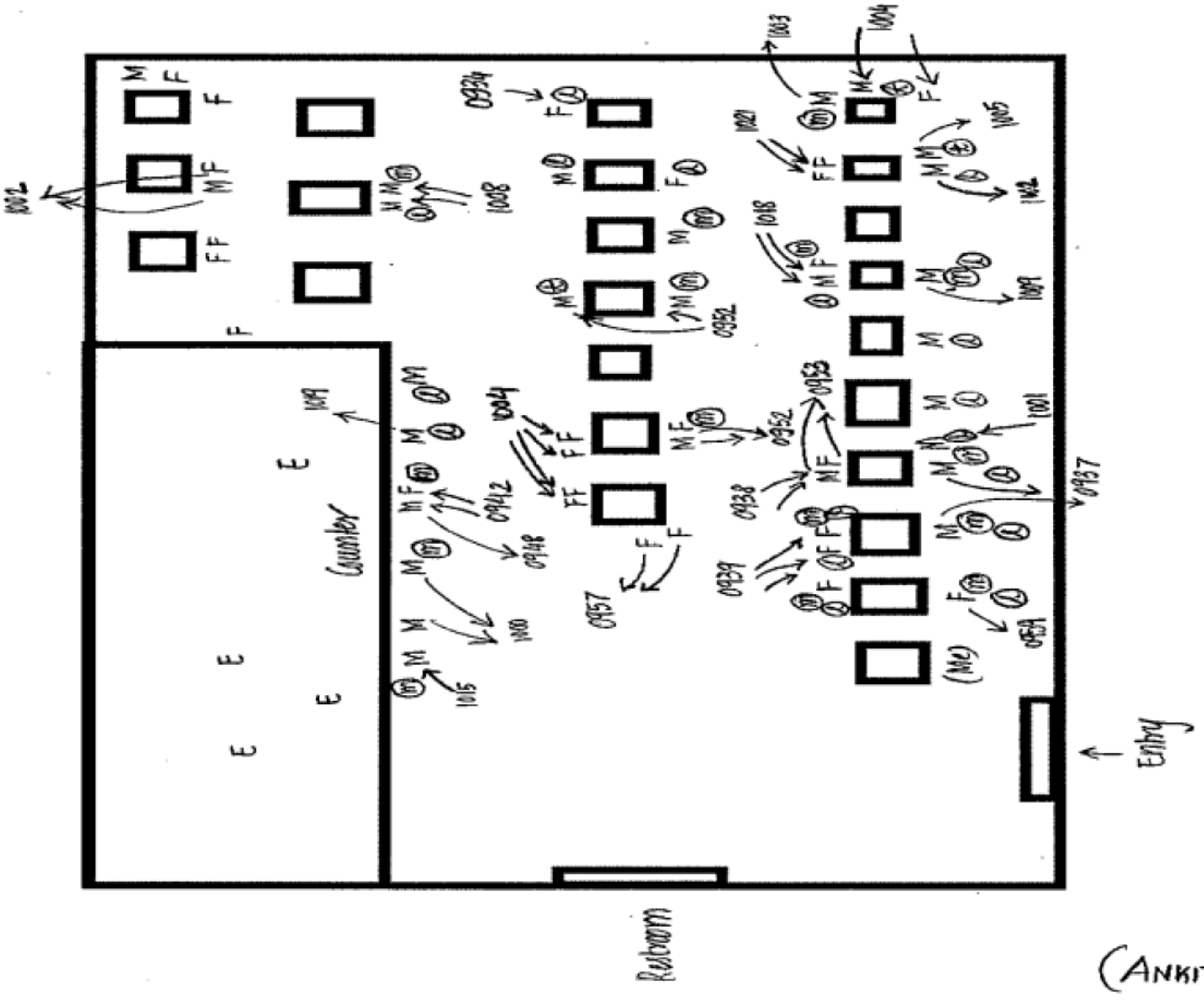
No. of Females: 24

No. of Employees: 4

No. of Mobiles: 15

No. of Laptops: 18

No. of Tablets: 3



M: Male

F: female

E: Employee

ⓜ: Mobile

Ⓣ: Tablet

Ⓛ: Laptop

(ANKIT BATTAU

Research Design- Phase 2

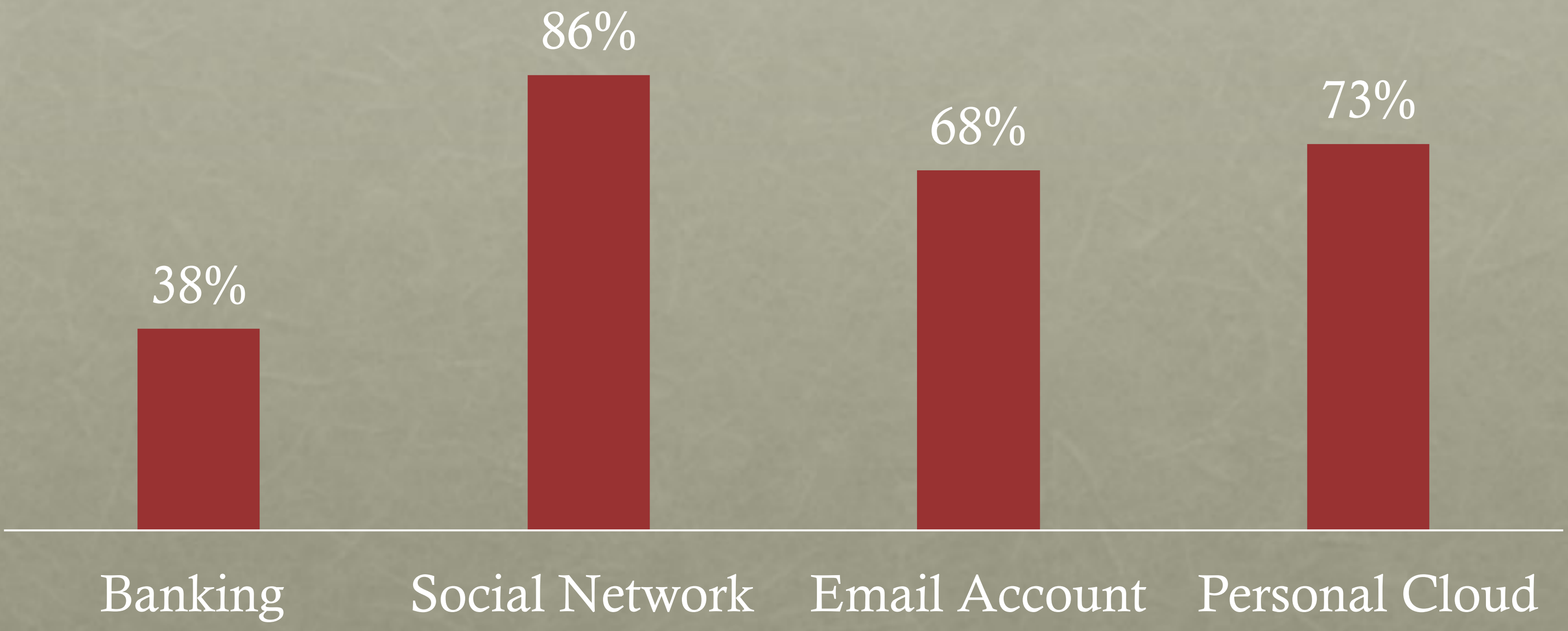
- Quasi-experimental one-group-post-test-only research design
  - 102 public WIFI locations in the state of MD and DC

Ethical and Privacy Considerations

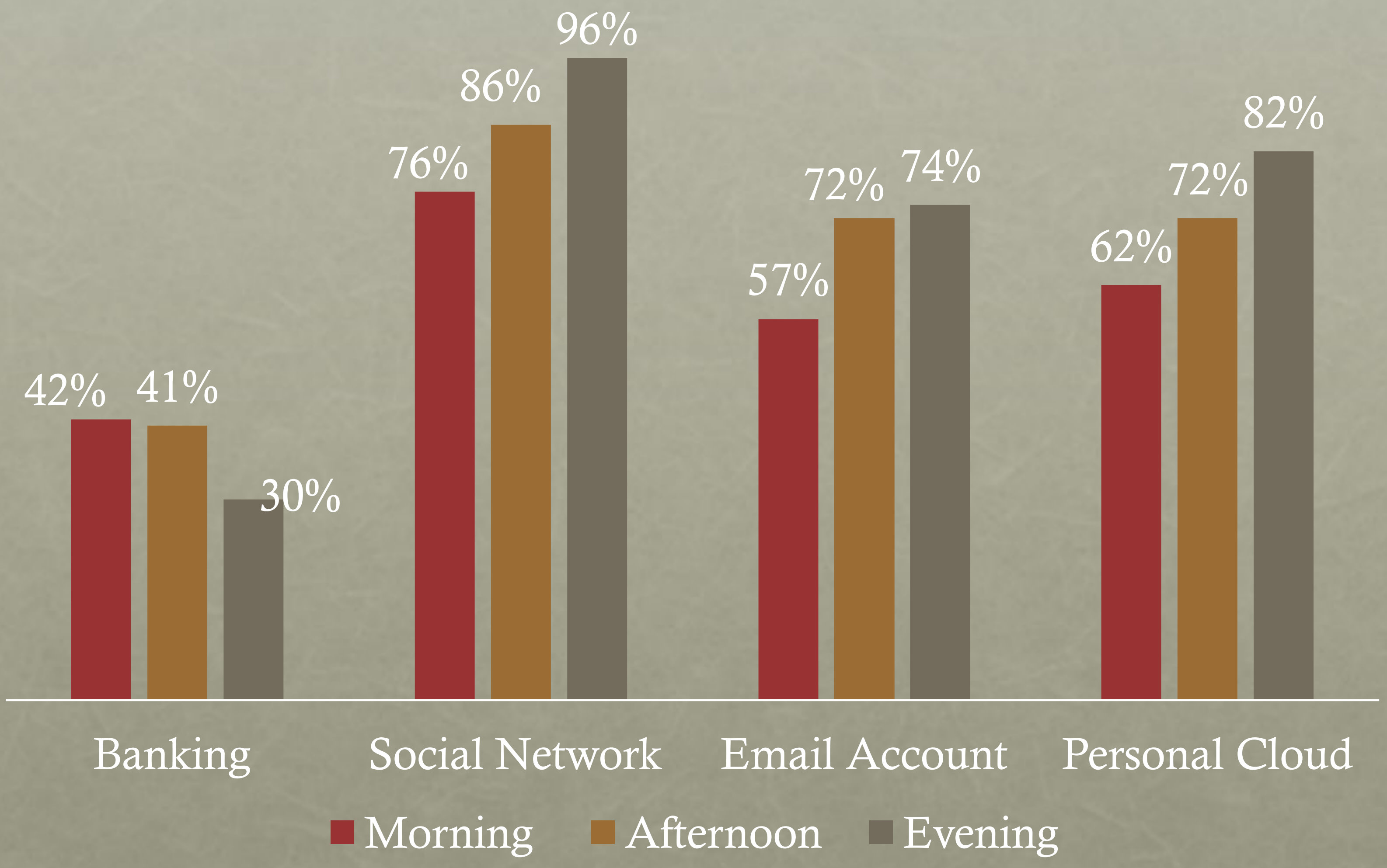
DEPENDENT VARIABLES

- Presence of email packets
- Presence of social network packets
- Presence of banking site packets
- Presence of e-commerce packets
- Presence of personal cloud packets

HOW COMMON AVOIDANCE FROM ACCESSING WEBSITES THAT HANDLE SENSITIVE INFORMATION AMONG WIFI NETWORKS IS?



Internet Packets Observed During 66 Sniffing Sessions on Public WiFi Hotspots in the DC Metropolitan Area Across Three Times of Day



Does uncertainty regarding the owner of a WiFi network shape users’ avoidance from accessing websites that handle sensitive information ?

Location Physical and Social Characteristics of Public WiFi Hotspots and Locations in which WiFi Networks Were Deployed

Location Physical and Social Characteristics	Extant Public WiFi Network	Honeypot WiFi Network
	Mean (SD)	Mean (SD)
Number of people	23.47 (12.30)	21.16 (17.39)
Number of males	11.25 (5.75)	10.66 (9.75)
Number of females	10.97 (6.18)	10.50 (8.42)
Number of customers	20.93 (11.49)	18.66 (16.39)
Number of employees	2.53 (1.69)	2.49 (2.14)
Number of mobile devices (observed)	8.22 (6.64)	2.77* (3.13)
Number of Laptops (observed)	4.31 (5.03)	2.70 (6.05)
% people sharing a table	61.88 (23.94)	69.77 (43.23)
% people sitting in adjacent tables	74.16 (25.98)	77.16 (56.85)

Census Tract Characteristics of Extant Public WiFi Hotspots and Honeypot WiFi Deployment Locations

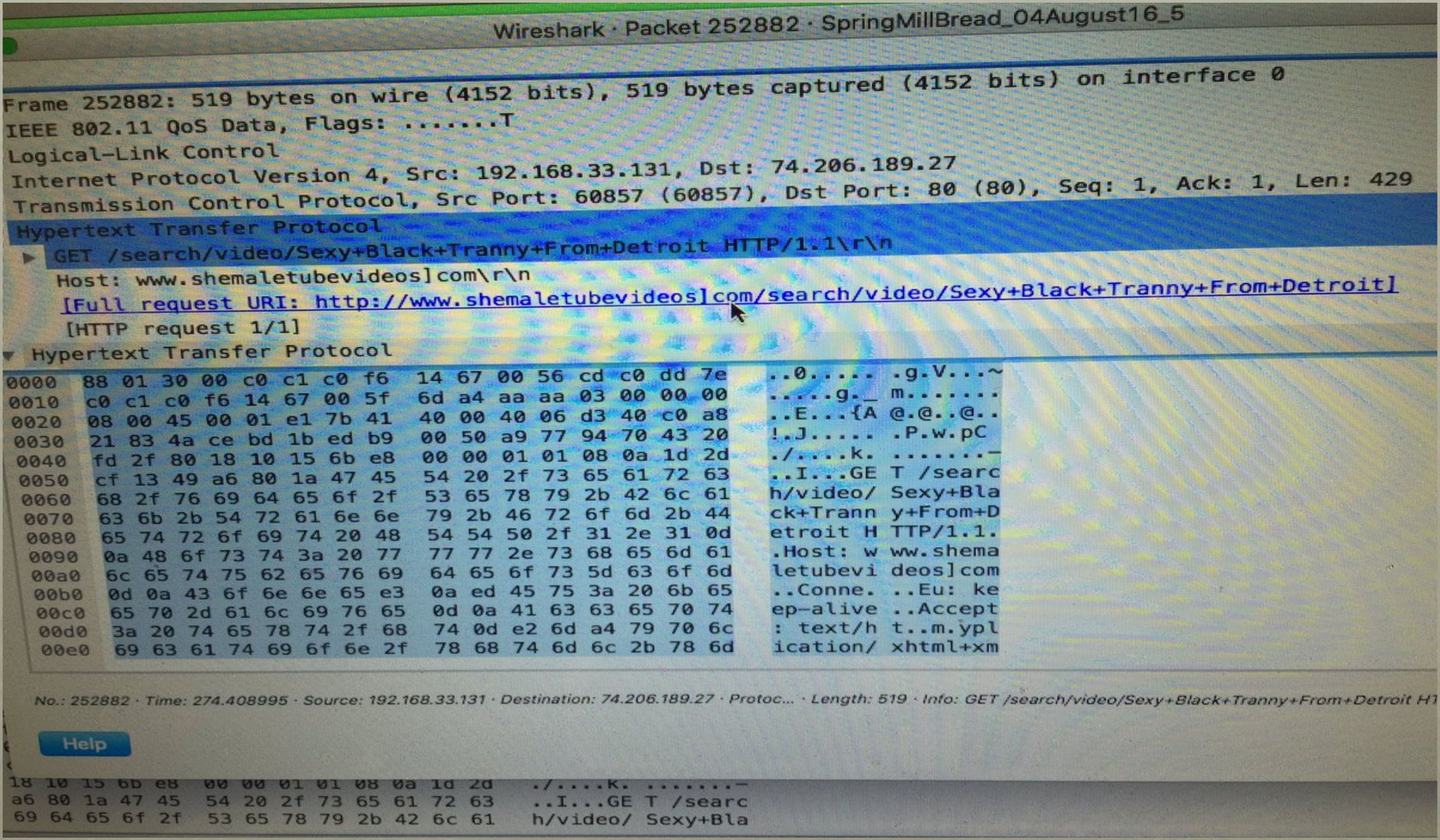
Neighborhood Characteristics	Extant Public WiFi Network	Honeypot WiFi Network
	Mean (SD)	Mean (SD)
Total population	3405 (1384.24)	4213 (2781.90)
Percent poverty	14.97 (9.09)	13.92 (13.26)
Percent unemployed	5.70 (4.00)	4.43 (3.10)
Percent foreign born	13.62 (10.42)	21.34* (14.46)
Percent female headed household	25.18 (18.03)	35.11 (61.17)
Percent living in the same house for more than 5 years	77.86 (9.40)	70.06** (11.07)

† $p<0.10$, * $p<0.05$, ** $p<0.01$

Proportion of Extant Public WiFi and Honeypot WiFi Network Locations in the DC Metropolitan Area with Different Types of Packets

Packets type	Proportion of extant Public WiFi Locations with Packets Observed (n=24)	Proportion of honeypot WiFi Locations with Packets Observed (n=31)
Advertisement	.83	.65**
Education	.41	.21**
News	.70	.27**
Sport	.41	.09**
Video streaming	.67	.23**

* p<0.05, ** p<0.01



Wireshark · Packet 252882 · SpringMillBread_04August16_5

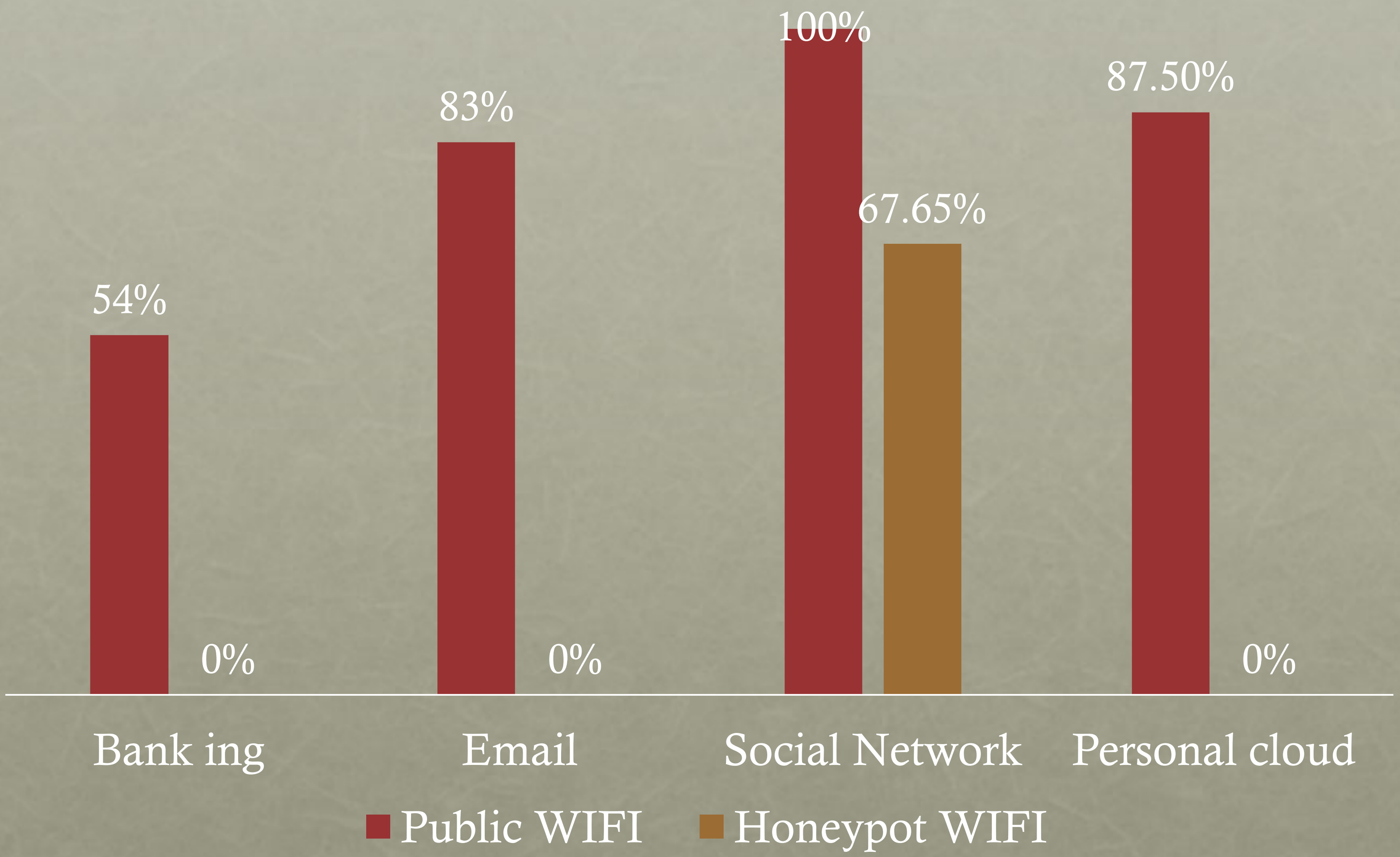
```
Frame 252882: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits) on interface 0
IEEE 802.11 QoS Data, Flags: .......T
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.33.131, Dst: 74.206.189.27
Transmission Control Protocol, Src Port: 60857 (60857), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 429
Hypertext Transfer Protocol
 ▶ GET /search/video/Sexy+Black+Tranny+From+Detroit HTTP/1.1\r\n
    Host: www.shemaletubevideos]com\r\n
    [Full request URI: http://www.shemaletubevideos]com/search/video/Sexy+Black+Tranny+From+Detroit]
    [HTTP request 1/1]
▼ Hypertext Transfer Protocol
```

```
0000  88 01 30 00 c0 c1 c0 f6  14 67 00 56 cd c0 dd 7e   ..0..... .g.V...~
0010  c0 c1 c0 f6 14 67 00 5f  6d a4 aa aa 03 00 00 00   .....g._ m.......
0020  08 00 45 00 01 e1 7b 41  40 00 40 06 d3 40 c0 a8   ..E...{A @.@..@..
0030  21 83 4a ce bd 1b ed b9  00 50 a9 77 94 70 43 20   !.J..... .P.w.pC
0040  fd 2f 80 18 10 15 6b e8  00 00 01 01 08 0a 1d 2d   ./....k. .......-
0050  cf 13 49 a6 80 1a 47 45  54 20 2f 73 65 61 72 63   ..I...GE T /searc
0060  68 2f 76 69 64 65 6f 2f  53 65 78 79 2b 42 6c 61   h/video/ Sexy+Bla
0070  63 6b 2b 54 72 61 6e 6e  79 2b 46 72 6f 6d 2b 44   ck+Trann y+From+D
0080  65 74 72 6f 69 74 20 48  54 54 50 2f 31 2e 31 0d   etroit H TTP/1.1.
0090  0a 48 6f 73 74 3a 20 77  77 77 2e 73 68 65 6d 61   .Host: w ww.shema
00a0  6c 65 74 75 62 65 76 69  64 65 6f 73 5d 63 6f 6d   letubevi deos]com
00b0  0d 0a 43 6f 6e 6e 65 e3  0a ed 45 75 3a 20 6b 65   ..Conne. ..Eu: ke
00c0  65 70 2d 61 6c 69 76 65  0d 0a 41 63 63 65 70 74   ep-alive ..Accept
00d0  3a 20 74 65 78 74 2f 68  74 0d e2 6d a4 79 70 6c   : text/h t..m.ypl
00e0  69 63 61 74 69 6f 6e 2f  78 68 74 6d 6c 2b 78 6d   ication/ xhtml+xm
```

No.: 252882 · Time: 274.408995 · Source: 192.168.33.131 · Destination: 74.206.189.27 · Protoc... · Length: 519 · Info: GET /search/video/Sexy+Black+Tranny+From+Detroit HT

```
18 10 15 6b e8  00 00 01 01 08 0a 1d 2d   ./....k. .......-
a6 80 1a 47 45  54 20 2f 73 65 61 72 63   ..I...GE T /searc
69 64 65 6f 2f  53 65 78 79 2b 42 6c 61   h/video/ Sexy+Bla
```

Internet Packets Observed on 24 Public WiFi Locations and 34 Honeypot WiFi Networks



CONCLUSIONS

- Although online avoidance strategy is rare among public WiFi users' in the context of social media, email, and personal cloud services, it appears to be quite common with respect to banking websites.

- Moreover, uncertainty regarding the WiFi network's legal owner and operator is associated with an increased likelihood of avoiding websites that handle sensitive information

David Maimon
Email: dmaimon@umd.edu
Website: www.davidmaimon.net
Twitter: @david_maimon