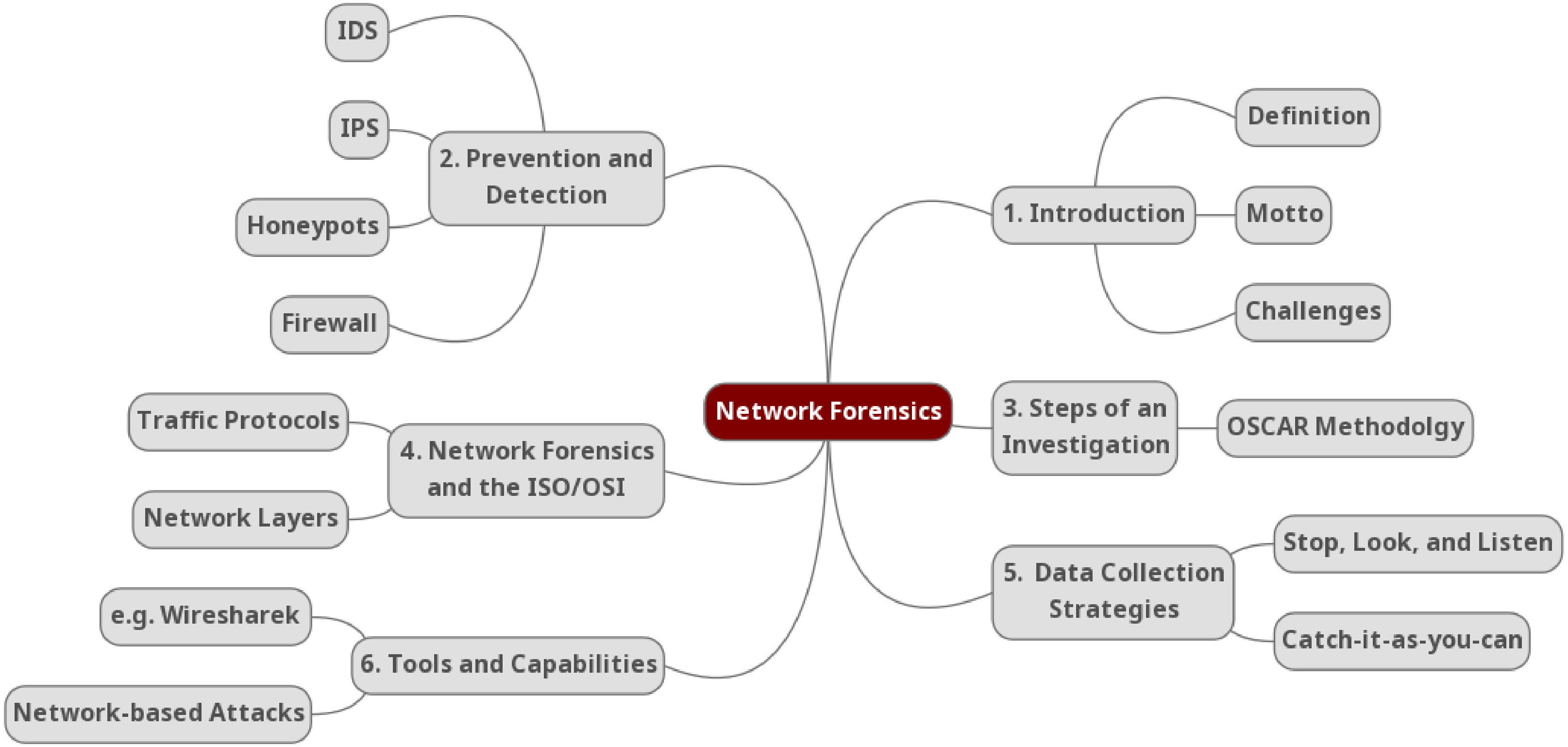
ulm university universität ulm

Chapter 6: Network Forensics

Introduction to Digital Forensics

Fröhlich, Hosh

http://cdn2.hubspot.net/hubfs/440597/network.png



- Network Forensics
  - 1. Introduction
    - Definition
    - Motto
    - Challenges
  - 2. Prevention and Detection
    - IDS
    - IPS
    - Honeypots
    - Firewall
  - 3. Steps of an Investigation
    - OSCAR Methodolgy
  - 4. Network Forensics and the ISO/OSI
    - Traffic Protocols
    - Network Layers
  - 5. Data Collection Strategies
    - Stop, Look, and Listen
    - Catch-it-as-you-can
  - 6. Tools and Capabilities
    - e.g. Wiresharek
    - Network-based Attacks

Literature

- *Network Forensics: Tracking Hackers through Cyberspace*
  - https://news.asis.io/sites/default/files/Network%20Forensics%202012.pdf
- *A Graph Based Approach Toward Network Forensics Analysis*
  - *https://users.cs.fiu.edu/~fortega/df/research/a4-wang.pdf*
- *Network forensics based on fuzzy logic and expert system*
  - *https://www.researchgate.net/publication/221433907_A_Fuzzy_Expert_System_for_Network_Forensics*
- PyFlag – An advanced network forensic framework
  - https://www.dfrws.org/sites/default/files/session-files/paper-pyflag_-_an_advanced_network_forensic_framework.pdf

Network Forensics

“The capturing, recording, and analysis of network packets to determine the source of a network breach.”

Motto

“An ounce of prevention is worth a pound of detection”.

Prevention and Detection

- IDS
- IPS
- Firewall
- Honeypots

IDS

Intrusion
Detection
System

IPS

Intrusion
Prevention
System

Honeypots

https://images.techhive.com/images/article/2015/09/honey_pot-100613200-primary.idge.jpg

OSCAR

Obtain information

Strategise

Collect evidence

Analyse

Report

Obtain information

Strategise

Collect evidence

Analyse

Report

Traffic Protocols
Network Layers

Forensics and the ISO/OSI Layers

__________ (Layer 1)

__________ (Layer 2)

__________ (Layer 3)

__________ (Layer 4)

__________ (Layer 5)

__________ (Layer 6)

__________ (Layer 7)

Forensics and the ISO/OSI Layers

- Physical (Layer 1)
- Data-Link (Layer 2)
- Network (Layer 3)
- Transport (Layer 4)
- Session (Layer 5)
- Presentation (Layer 6)
- Application (Layer 7)

Data/Traffic Collection Strategies

"Stop, Look, Listen"

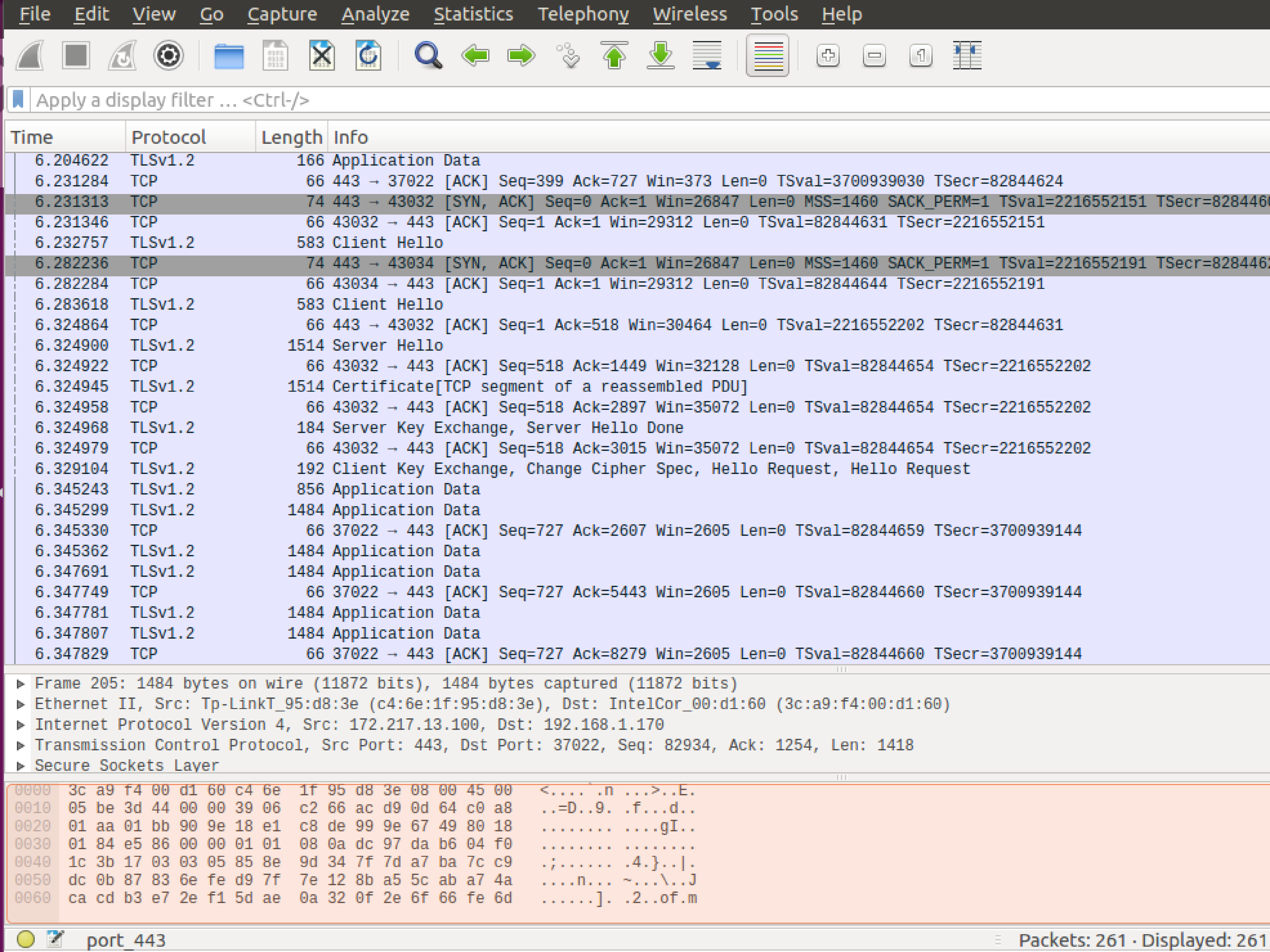
"Catch-it-as-you-can"

Stop, Look, Listen

- Only store data needed
- Analyse/filter in real-time
- Pros: Fair storage capacity
- Cons: High performance CPU

Catch-it-as-you-can

- Store all captured data
- Analyse/filter post-mortem
- Pros: Exhaustive data
- Cons: Large storage capacity


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

```
Time        Protocol   Length Info
  6.204622  TLSv1.2      166 Application Data
  6.231284  TCP           66 443 → 37022 [ACK] Seq=399 Ack=727 Win=373 Len=0 TSval=3700939030 TSecr=82844624
  6.231313  TCP           74 443 → 43032 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2216552151 TSecr=828446
  6.231346  TCP           66 43032 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=82844631 TSecr=2216552151
  6.232757  TLSv1.2      583 Client Hello
  6.282236  TCP           74 443 → 43034 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2216552191 TSecr=828446
  6.282284  TCP           66 43034 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=82844644 TSecr=2216552191
  6.283618  TLSv1.2      583 Client Hello
  6.324864  TCP           66 443 → 43032 [ACK] Seq=1 Ack=518 Win=30464 Len=0 TSval=2216552202 TSecr=82844631
  6.324900  TLSv1.2     1514 Server Hello
  6.324922  TCP           66 43032 → 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=82844654 TSecr=2216552202
  6.324945  TLSv1.2     1514 Certificate[TCP segment of a reassembled PDU]
  6.324958  TCP           66 43032 → 443 [ACK] Seq=518 Ack=2897 Win=35072 Len=0 TSval=82844654 TSecr=2216552202
  6.324968  TLSv1.2      184 Server Key Exchange, Server Hello Done
  6.324979  TCP           66 43032 → 443 [ACK] Seq=518 Ack=3015 Win=35072 Len=0 TSval=82844654 TSecr=2216552202
  6.329104  TLSv1.2      192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
  6.345243  TLSv1.2      856 Application Data
  6.345299  TLSv1.2     1484 Application Data
  6.345330  TCP           66 37022 → 443 [ACK] Seq=727 Ack=2607 Win=2605 Len=0 TSval=82844659 TSecr=3700939144
  6.345362  TLSv1.2     1484 Application Data
  6.347691  TLSv1.2     1484 Application Data
  6.347749  TCP           66 37022 → 443 [ACK] Seq=727 Ack=5443 Win=2605 Len=0 TSval=82844660 TSecr=3700939144
  6.347781  TLSv1.2     1484 Application Data
  6.347807  TLSv1.2     1484 Application Data
  6.347829  TCP           66 37022 → 443 [ACK] Seq=727 Ack=8279 Win=2605 Len=0 TSval=82844660 TSecr=3700939144
```

```
▶ Frame 205: 1484 bytes on wire (11872 bits), 1484 bytes captured (11872 bits)
▶ Ethernet II, Src: Tp-LinkT_95:d8:3e (c4:6e:1f:95:d8:3e), Dst: IntelCor_00:d1:60 (3c:a9:f4:00:d1:60)
▶ Internet Protocol Version 4, Src: 172.217.13.100, Dst: 192.168.1.170
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 37022, Seq: 82934, Ack: 1254, Len: 1418
▶ Secure Sockets Layer
```

```
0000  3c a9 f4 00 d1 60 c4 6e  1f 95 d8 3e 08 00 45 00   <.... .n ...>..E.
0010  05 be 3d 44 00 00 39 06  c2 66 ac d9 0d 64 c0 a8   ..=D..9. .f...d..
0020  01 aa 01 bb 90 9e 18 e1  c8 de 99 9e 67 49 80 18   ........ ....gI..
0030  01 84 e5 86 00 00 01 01  08 0a dc 97 da b6 04 f0   ........ ........
0040  1c 3b 17 03 03 05 85 8e  9d 34 7f 7d a7 ba 7c c9   .;...... .4.}..|.
0050  dc 0b 87 83 6e fe d9 7f  7e 12 8b a5 5c ab a7 4a   ....n... ~...\..J
0060  ca cd b3 e7 2e f1 5d ae  0a 32 0f 2e 6f 66 fe 6d   ......]. .2..of.m
```

port_443 Packets: 261 · Displayed: 261

Challenges

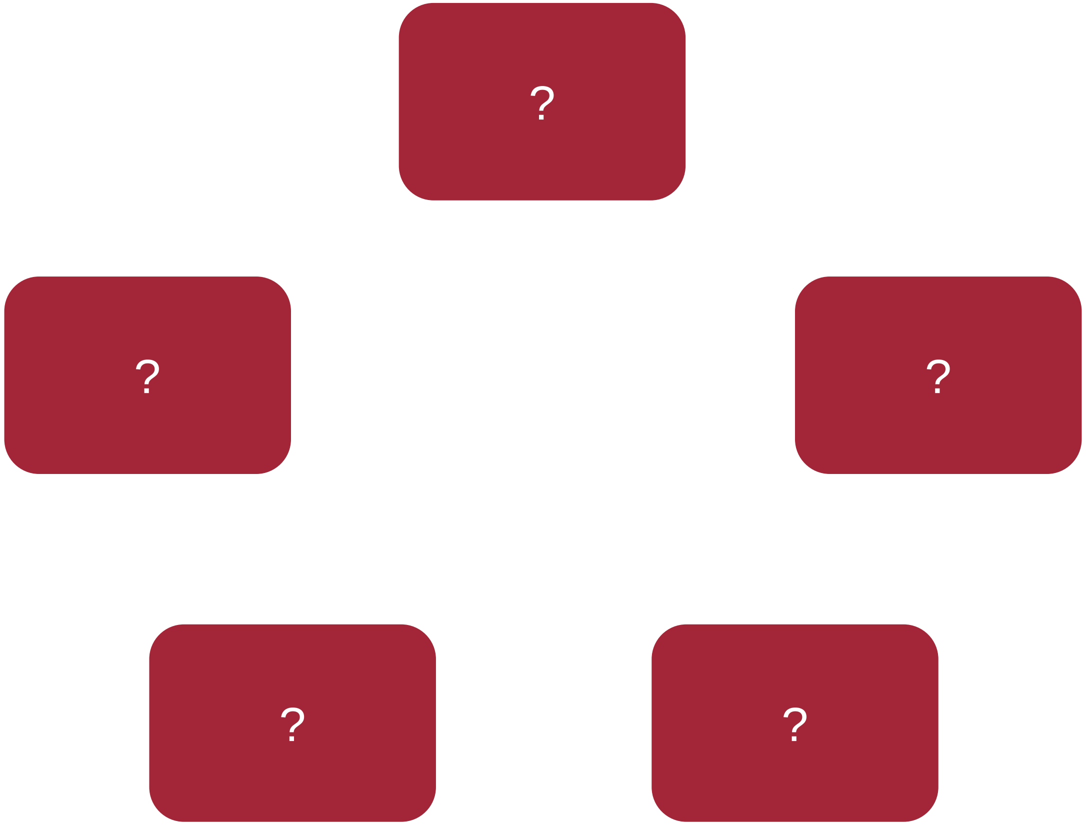
Challenges

- Data is changing constantly
- Pinpointing direct location of evidence is problematic
- Physical access to network devices is difficult
- No persistent storage in network devices
- Minimize investigation overhead on running network
- Legal aspect

Capabilites of Network Forensics Tools

- Network traffic capturing and analysis
- Evaluation of network performance
- Detection of anomalies
- Determination of used protocols
- Aggregation of multiple network sources
- Security investigations and incident response

Network-based attacks



?

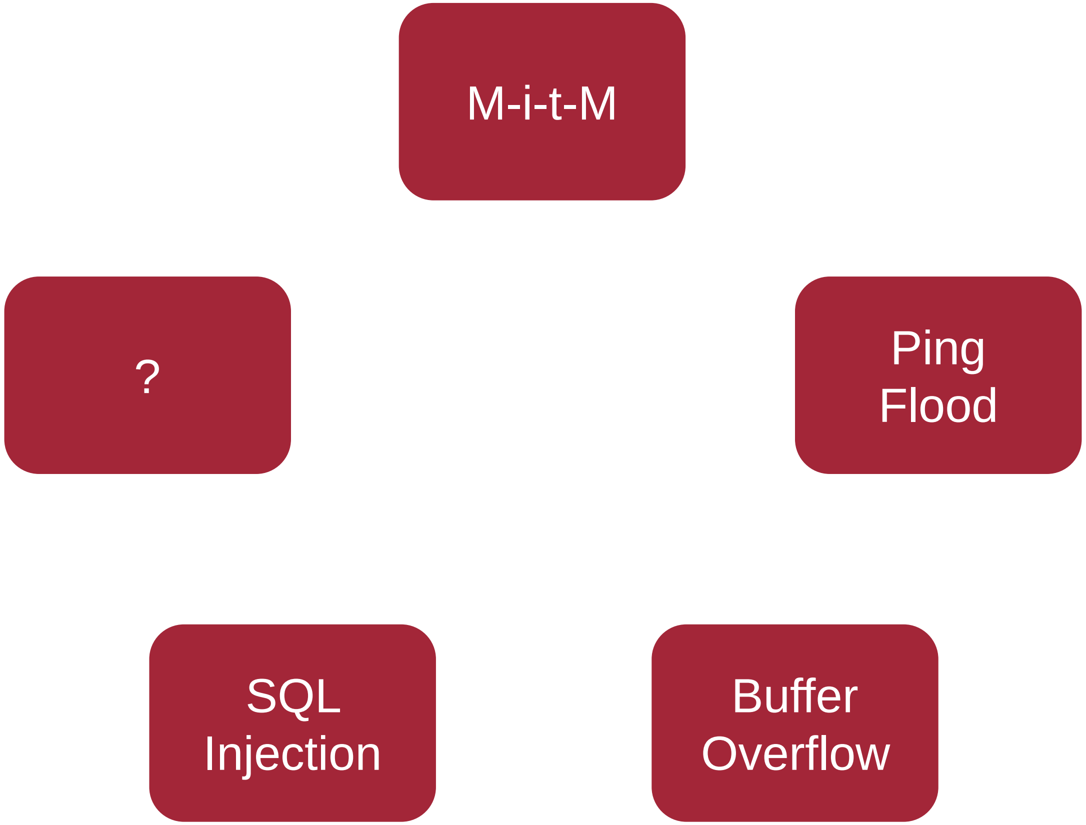
?

?

?

?

Network-based attacks



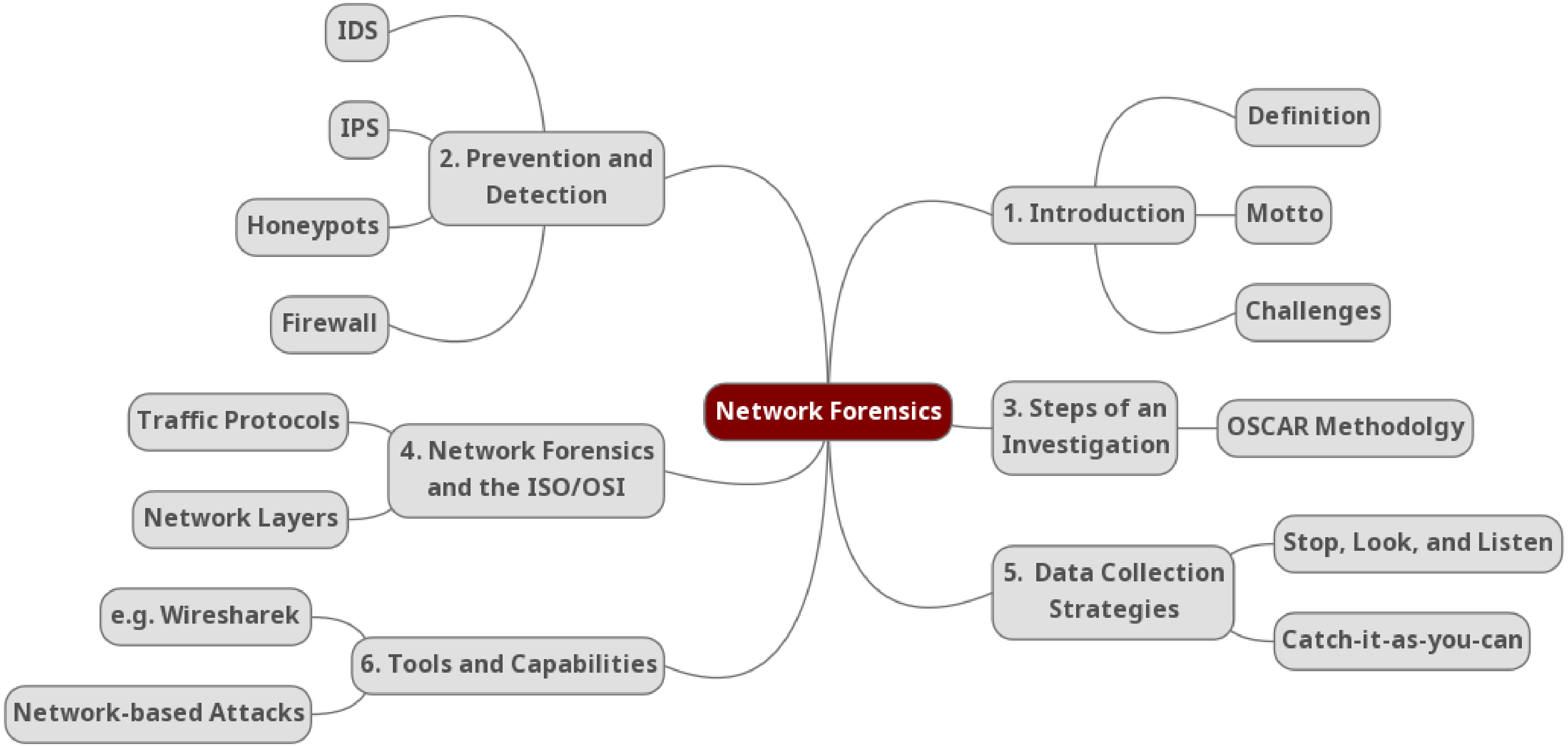
M-i-t-M

?

Ping Flood

SQL Injection

Buffer Overflow



Network Forensics

- 1. Introduction
  - Definition
  - Motto
  - Challenges
- 2. Prevention and Detection
  - IDS
  - IPS
  - Honeypots
  - Firewall
- 3. Steps of an Investigation
  - OSCAR Methodolgy
- 4. Network Forensics and the ISO/OSI
  - Traffic Protocols
  - Network Layers
- 5. Data Collection Strategies
  - Stop, Look, and Listen
  - Catch-it-as-you-can
- 6. Tools and Capabilities
  - e.g. Wiresharek
  - Network-based Attacks

ulm university universität uulm

Network Forensics

Introduction to Digital Forensics

Fröhlich, Hosh

http://cdn2.hubspot.net/hubfs/440597/network.png