Digital Forensics & Packet Analysis

UBNetDef, Fall 2021
Week 14

About Me

- Education
  - Bachelor of Science, Business Administration
  - Master of Science, MIS
- Security Experience
  - Consultant/Senior Consultant, Cyber Risk services, Deloitte
  - Lead Cybersecurity Consultant and vCISO, Loptr LLC
- Professional Affiliations
  - ISC^2; Certified Information Systems Security Professional (CISSP)
  - Buffalo Electronic Crimes Task Force
- Publications:
  - Vulnerability Assessment (ISACA, 2017)
- Hats worn:
  - Virtual CISO
  - Project Manager
  - Security Analyst
  - Security Monitoring Analyst
  - Security Architect
  - Software Developer

Dominic Sellitto, CISSP

Clinical Assistant Professor
Program Director, MS Business Analytics

Skills

NetDef

Agenda

1. Digital Forensics Overview
2. Subdomains within Digital Forensics
3. Network Forensics Overview
4. Wireshark Exercise 1
5. Wireshark Exercise 2
6. Homework

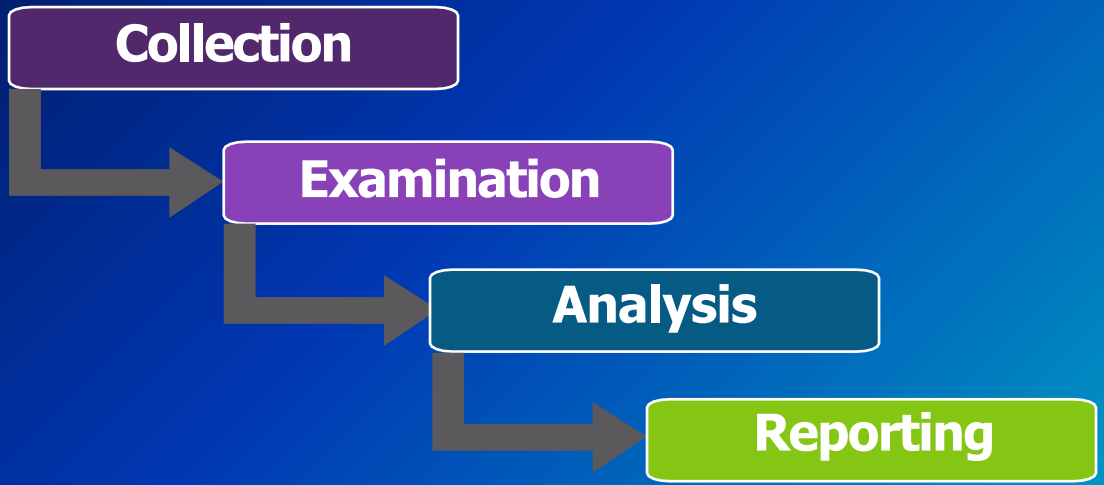
What is Digital Forensics

- Digital Forensics is “the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.”
  - NIST SP-800-86, Guide to Integrating Forensic Techniques Into Incident Response (Pg. 15)
- Digital Forensics may also be referred to as:
  - Computer and Network Forensics
  - Data Forensics

NetDef

Phases of the Forensics Process

- **NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response** describes the 4 phases of the forensics process as follows:

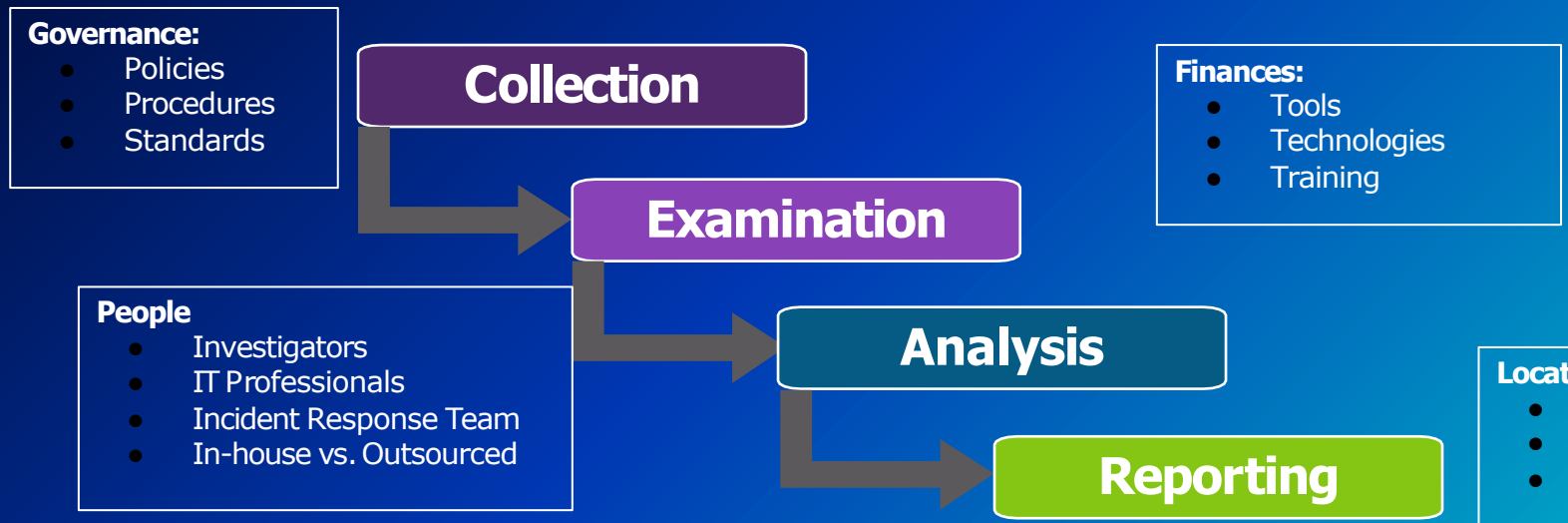


Source: NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

NetDef

Enabling Factors

- In order to repeatedly execute the process, you need some things...



Source: NIST 800-86: Guide to Integrating Forensic Techniques into Incident Response

NetDef

Forensic Areas of Practice

- You might just think of forensics as examining hard drives, but it's much more than that:


Media Forensics


Malware Analysis


Memory Forensics


Network Forensics


Mobile Forensics


Cloud Forensics


Email Forensics


Digital Media Manipulation


IoT Forensics


Automobile Forensics

Digital Media Manipulation

- Which of these is fake?

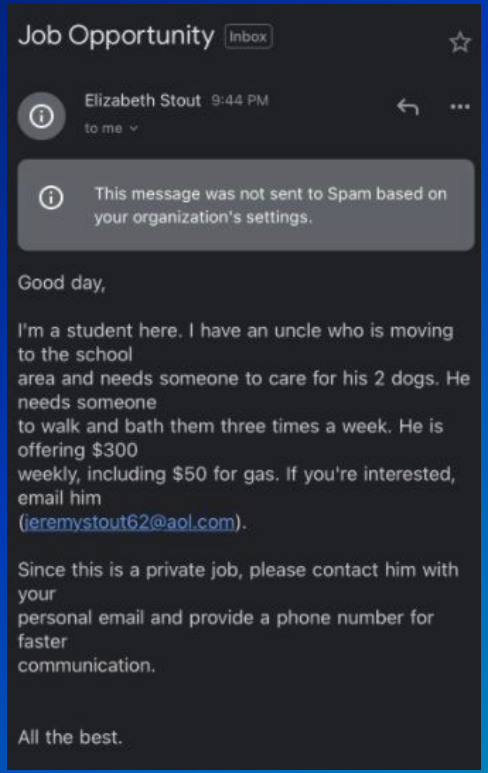
NetDef

Malware Analysis...

- What's that program ***really*** doing?

NetDef

Email Forensics...



Job Opportunity Inbox

Elizabeth Stout 9:44 PM
to me

This message was not sent to Spam based on your organization's settings.

Good day,

I'm a student here. I have an uncle who is moving to the school
area and needs someone to care for his 2 dogs. He needs someone
to walk and bath them three times a week. He is offering $300
weekly, including $50 for gas. If you're interested, email him
(jeremystout62@aol.com).

Since this is a private job, please contact him with your
personal email and provide a phone number for faster
communication.

All the best.

NetDef

Network Forensics

- **Packets** contain all of the information being sent across a network, including the source and destination machine, protocol being used, and the actual data being sent
- **Network logs** are records of network events - they tell you that something happened over the network (like source, destination, protocol) but do not contain the actual data that was sent

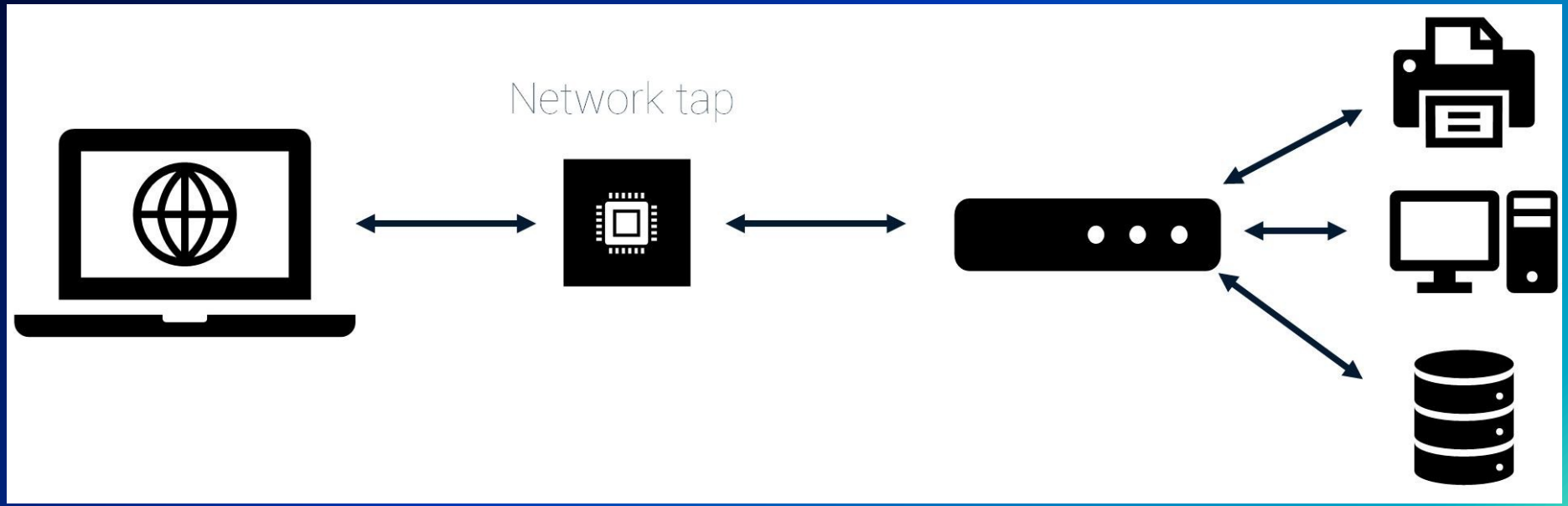
NetDef

Network Forensics- Capturing Packets

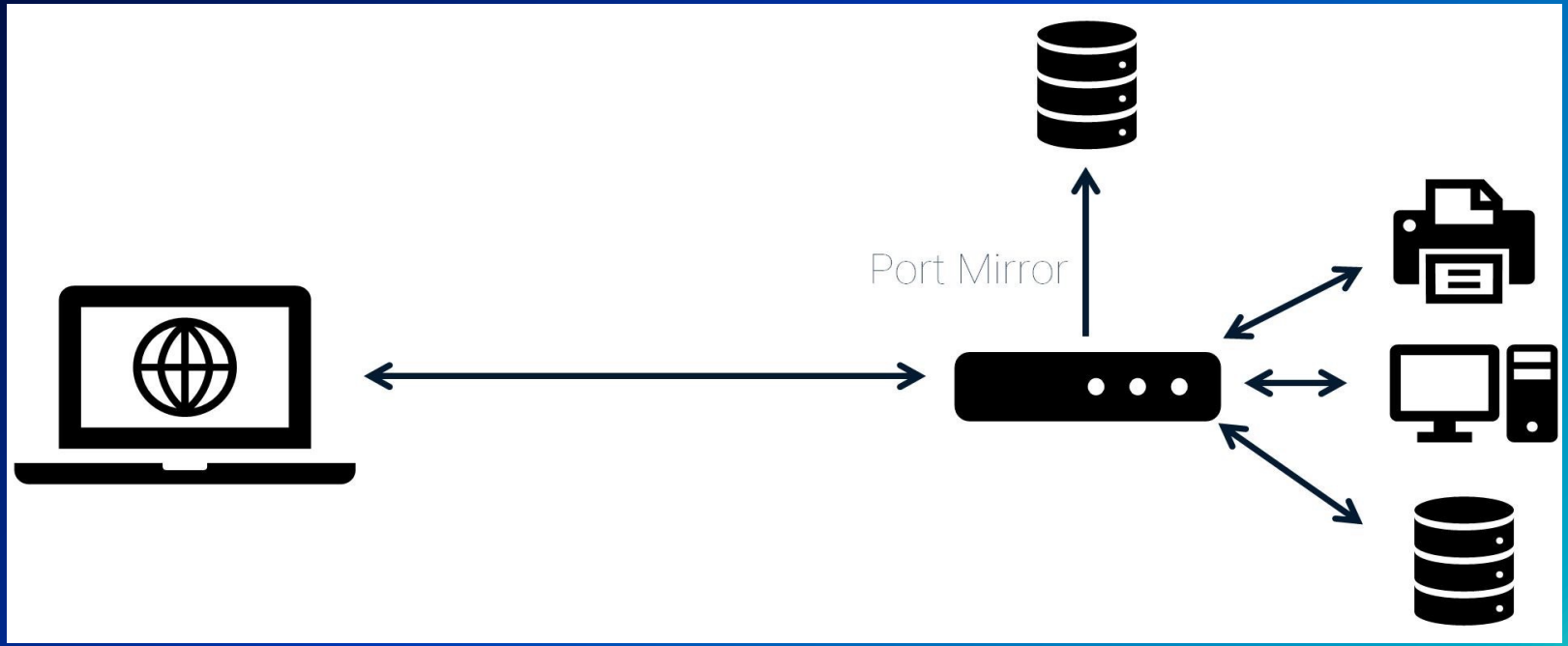
Packets can be captured using a variety of methods:

- Network tap
  - A device placed between two networked devices that captures traffic flowing between
- Port Mirroring
  - Sends “copies” of packets flowing through a network switch to a specified location (e.g., packet capture server)
- Wireless Sniffing
  - Listens over a wireless network for traffic and captures packets

Network Forensics- Capturing Packets



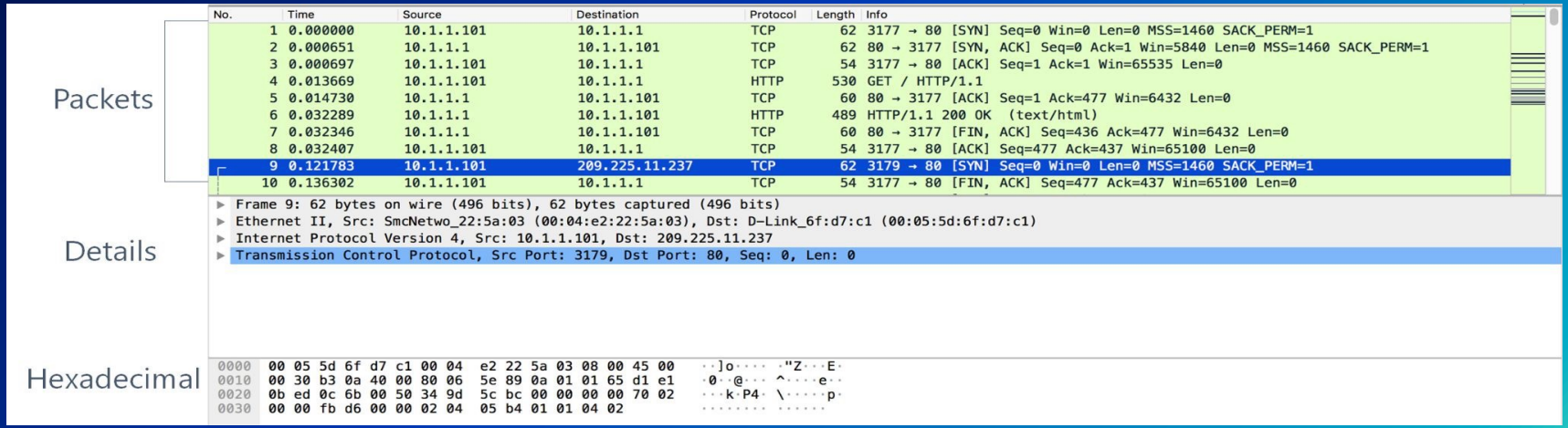
Network Forensics- Capturing Packets

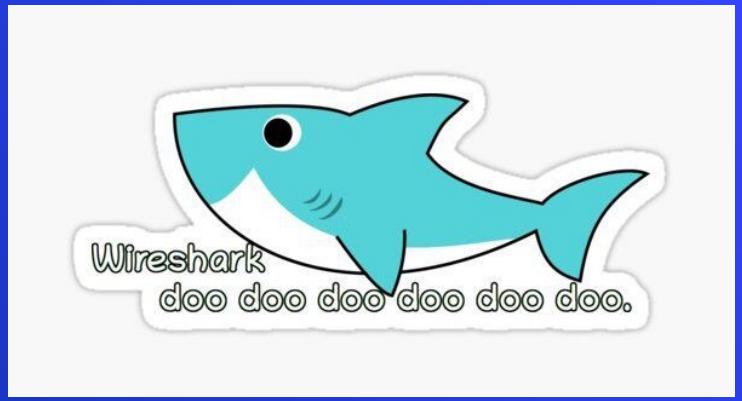


Network Forensics- Capturing Packets

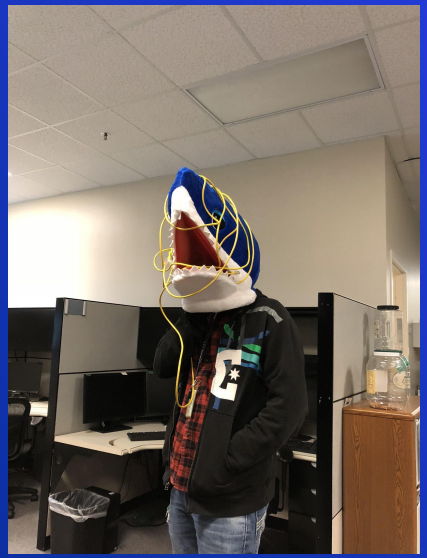
Packets: Examination and Analysis

- You can use a packet analyzer, like **Wireshark**, to dive into packets to identify what data was transmitted over a network




Wireshark
doo doo doo doo doo doo.


PCAP
OR IT
DIDN'T
Happen

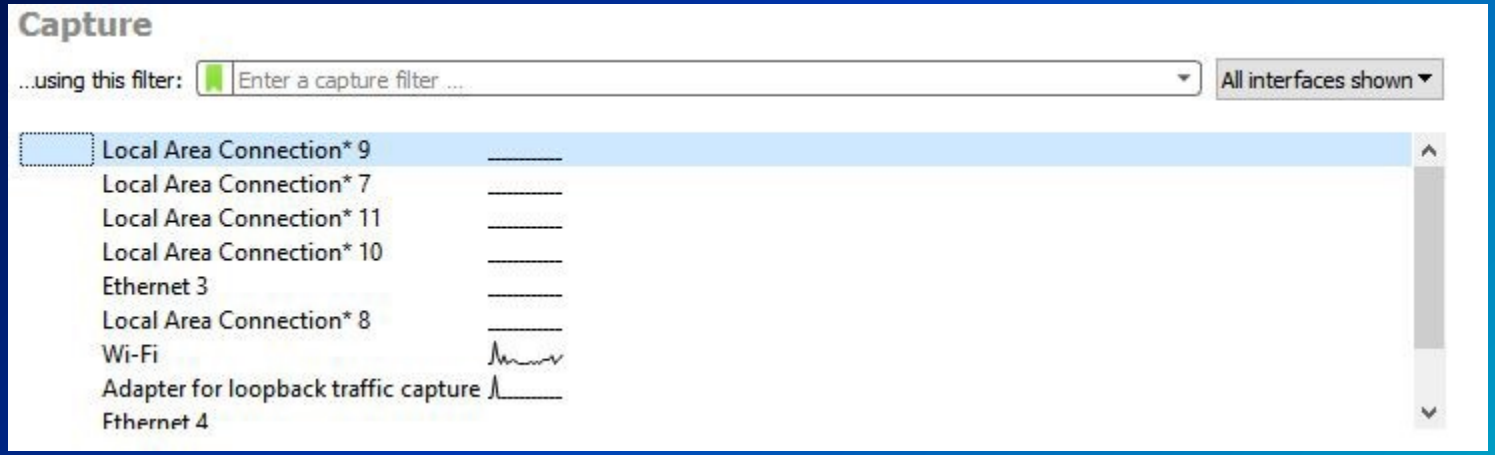


Break Time!

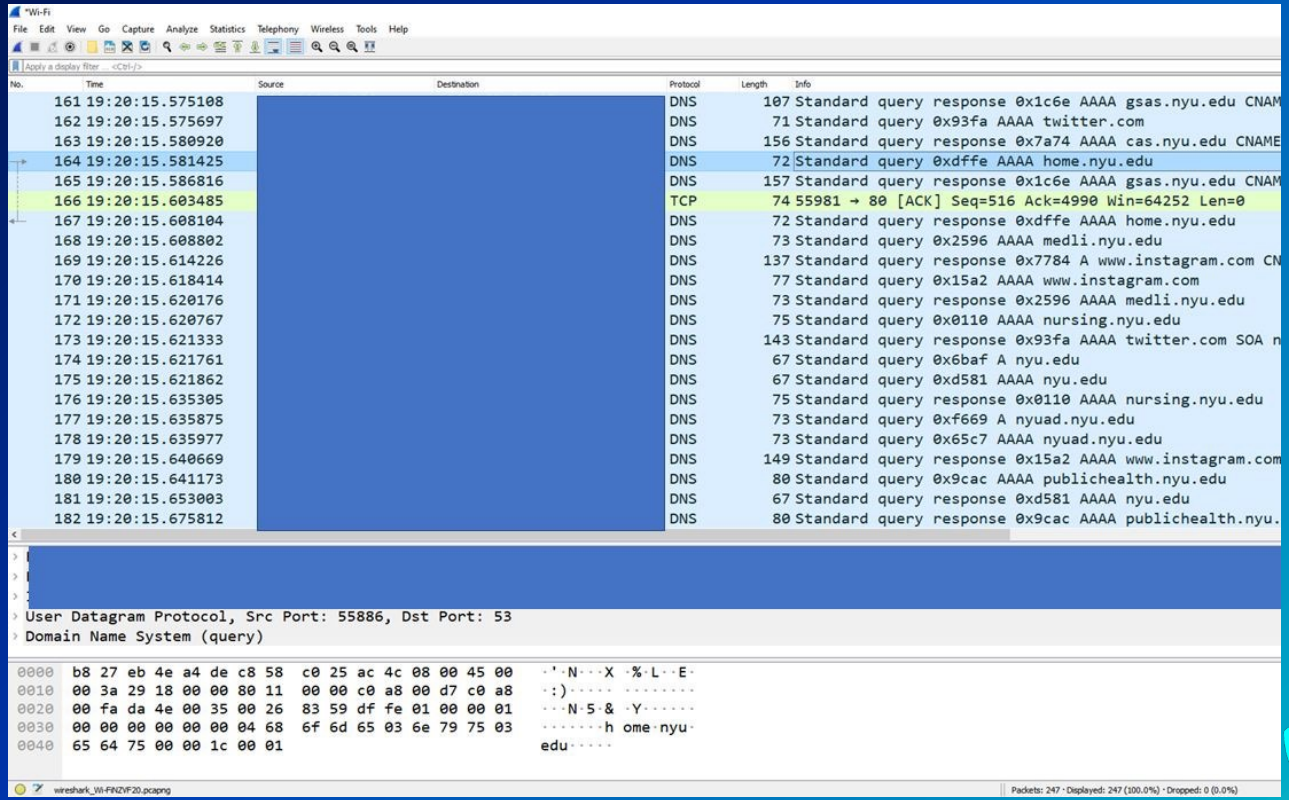

WIRESHARK

Demo: Introduction to Wireshark

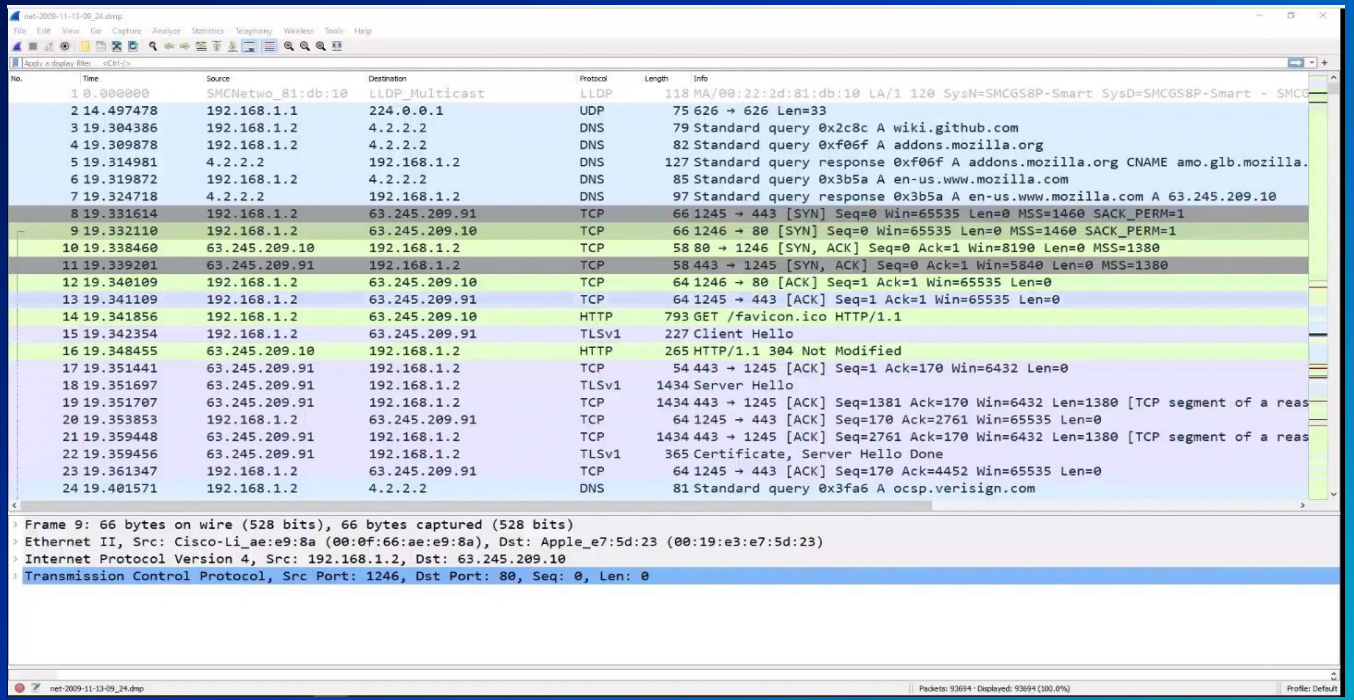
Capturing packets from your network adapter



Stopping your packet capture and examining results...



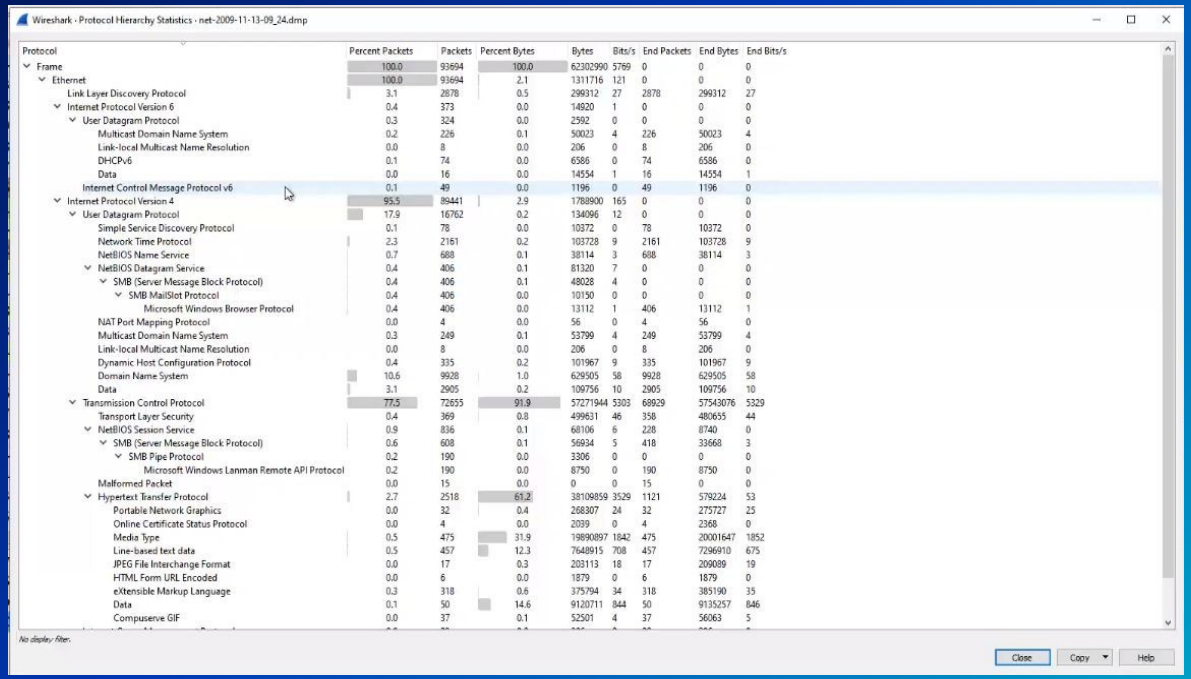
Overview of the packet list



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	SMCNetwo_81:db:10	LLDP_Multicast	LLDP	118	MA/00:22:2d:81:db:10 LA/1 120 SysN=SMCGS8P-Smart SysD=SMCGS8P-Smart - SMCG
2	14.497478	192.168.1.1	224.0.0.1	UDP	75	626 → 626 Len=33
3	19.304386	192.168.1.2	4.2.2.2	DNS	79	Standard query 0x2c8c A wiki.github.com
4	19.309878	192.168.1.2	4.2.2.2	DNS	82	Standard query 0xf06f A addons.mozilla.org
5	19.314981	4.2.2.2	192.168.1.2	DNS	127	Standard query response 0xf06f A addons.mozilla.org CNAME amo.glb.mozilla.
6	19.319872	192.168.1.2	4.2.2.2	DNS	85	Standard query 0x3b5a A en-us.www.mozilla.com
7	19.324718	4.2.2.2	192.168.1.2	DNS	97	Standard query response 0x3b5a A en-us.www.mozilla.com A 63.245.209.10
8	19.331614	192.168.1.2	63.245.209.91	TCP	66	1245 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
9	19.332110	192.168.1.2	63.245.209.10	TCP	66	1246 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
10	19.338460	63.245.209.10	192.168.1.2	TCP	58	80 → 1246 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1380
11	19.339201	63.245.209.91	192.168.1.2	TCP	58	443 → 1245 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
12	19.340109	192.168.1.2	63.245.209.10	TCP	64	1246 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
13	19.341109	192.168.1.2	63.245.209.91	TCP	64	1245 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
14	19.341856	192.168.1.2	63.245.209.10	HTTP	793	GET /favicon.ico HTTP/1.1
15	19.342354	192.168.1.2	63.245.209.91	TLSv1	227	Client Hello
16	19.348455	63.245.209.10	192.168.1.2	HTTP	265	HTTP/1.1 304 Not Modified
17	19.351441	63.245.209.91	192.168.1.2	TCP	54	443 → 1245 [ACK] Seq=1 Ack=170 Win=6432 Len=0
18	19.351697	63.245.209.91	192.168.1.2	TLSv1	1434	Server Hello
19	19.351707	63.245.209.91	192.168.1.2	TCP	1434	443 → 1245 [ACK] Seq=1381 Ack=170 Win=6432 Len=1380 [TCP segment of a reas
20	19.353853	192.168.1.2	63.245.209.91	TCP	64	1245 → 443 [ACK] Seq=170 Ack=2761 Win=65535 Len=0
21	19.359448	63.245.209.91	192.168.1.2	TCP	1434	443 → 1245 [ACK] Seq=2761 Ack=170 Win=6432 Len=1380 [TCP segment of a reas
22	19.359456	63.245.209.91	192.168.1.2	TLSv1	365	Certificate, Server Hello Done
23	19.361347	192.168.1.2	63.245.209.91	TCP	64	1245 → 443 [ACK] Seq=170 Ack=4452 Win=65535 Len=0
24	19.401571	192.168.1.2	4.2.2.2	DNS	81	Standard query 0x3fa6 A ocsp.verisign.com

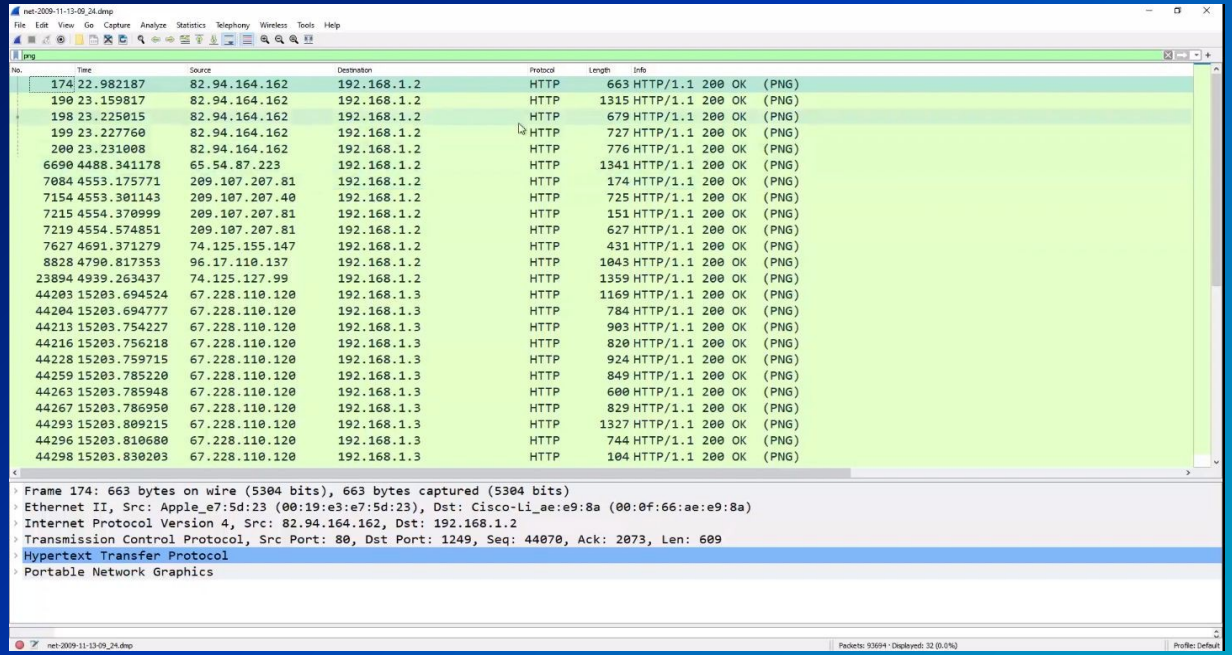
```
Frame 9: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco-Li_ae:e9:8a (00:0f:66:ae:e9:8a), Dst: Apple_e7:5d:23 (00:19:e3:e7:5d:23)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 63.245.209.10
Transmission Control Protocol, Src Port: 1246, Dst Port: 80, Seq: 0, Len: 0
```

Protocol hierarchy statistics

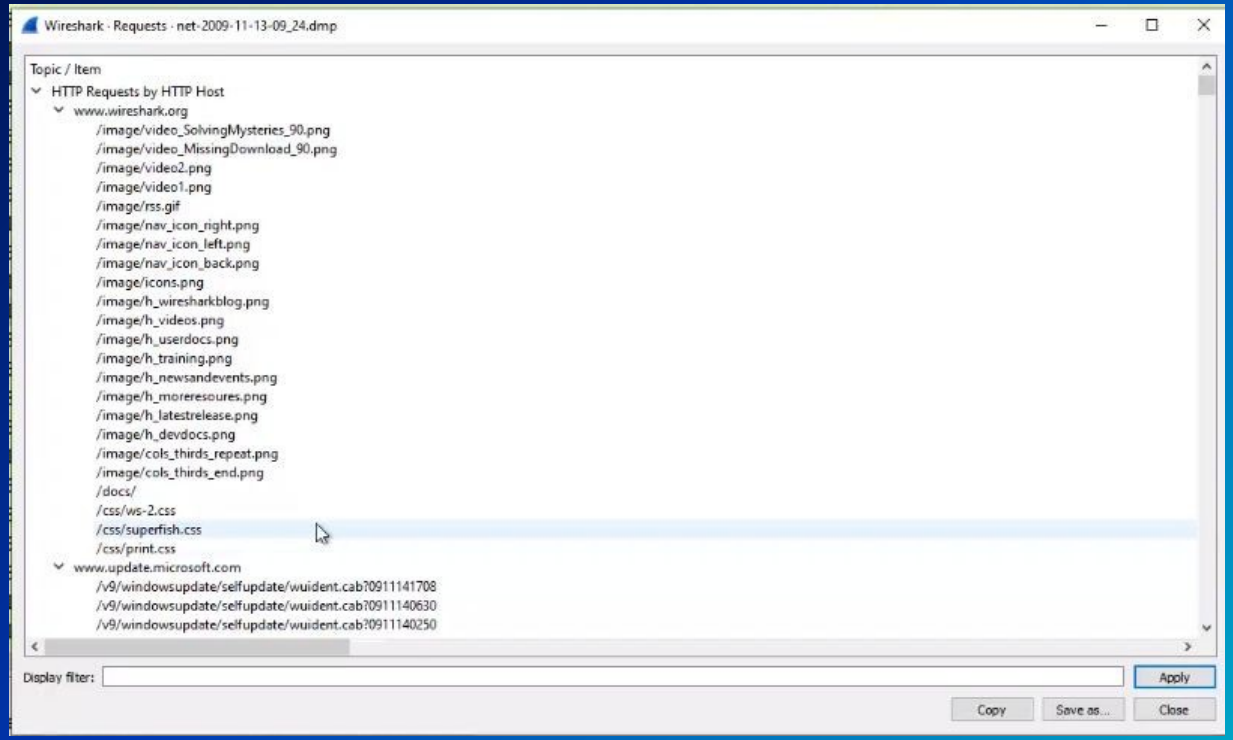


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	93694	100.0	62302990	5769	0	0	0
Ethernet	100.0	93694	2.1	1311716	121	0	0	0
Link Layer Discovery Protocol	3.1	2878	0.5	299312	27	2878	299312	27
Internet Protocol Version 6	0.4	373	0.0	14920	1	0	0	0
User Datagram Protocol	0.3	324	0.0	2592	0	0	0	0
Multicast Domain Name System	0.2	226	0.1	50023	4	226	50023	4
Link-local Multicast Name Resolution	0.0	8	0.0	206	0	8	206	0
DHCPv6	0.1	74	0.0	6586	0	74	6586	0
Data	0.0	16	0.0	14554	1	16	14554	1
Internet Control Message Protocol v6	0.1	49	0.0	1196	0	49	1196	0
Internet Protocol Version 4	95.5	89441	2.9	1788900	165	0	0	0
User Datagram Protocol	17.9	16762	0.2	134096	12	0	0	0
Simple Service Discovery Protocol	0.1	78	0.0	10372	0	78	10372	0
Network Time Protocol	2.3	2161	0.2	103728	9	2161	103728	9
NetBIOS Name Service	0.7	688	0.1	38114	3	688	38114	3
NetBIOS Datagram Service	0.4	406	0.1	81320	7	0	0	0
SMB (Server Message Block Protocol)	0.4	406	0.1	48028	4	0	0	0
SMB MailSlot Protocol	0.4	406	0.0	10150	0	0	0	0
Microsoft Windows Browser Protocol	0.4	406	0.0	13112	1	406	13112	1
NAT Port Mapping Protocol	0.0	4	0.0	56	0	4	56	0
Multicast Domain Name System	0.3	249	0.1	53799	4	249	53799	4
Link-local Multicast Name Resolution	0.0	8	0.0	206	0	8	206	0
Dynamic Host Configuration Protocol	0.4	335	0.2	101967	9	335	101967	9
Domain Name System	10.6	9928	1.0	629505	58	9928	629505	58
Data	3.1	2905	0.2	109756	10	2905	109756	10
Transmission Control Protocol	77.5	72655	91.9	57271944	5303	68929	57543076	5329
Transport Layer Security	0.4	369	0.8	499631	46	358	480655	44
NetBIOS Session Service	0.9	836	0.1	68106	6	228	8740	0
SMB (Server Message Block Protocol)	0.6	608	0.1	56934	5	418	33668	3
SMB Pipe Protocol	0.2	190	0.0	3306	0	0	0	0
Microsoft Windows Lanman Remote API Protocol	0.2	190	0.0	8750	0	190	8750	0
Malformed Packet	0.0	15	0.0	0	0	15	0	0
Hypertext Transfer Protocol	2.7	2518	61.2	38109859	3529	1121	579224	53
Portable Network Graphics	0.0	32	0.4	268307	24	32	275727	25
Online Certificate Status Protocol	0.0	4	0.0	2039	0	4	2368	0
Media Type	0.5	475	31.9	19890897	1842	475	20001647	1852
Line-based text data	0.5	457	12.3	7648915	708	457	7296910	675
JPEG File Interchange Format	0.0	17	0.3	203113	18	17	209089	19
HTML Form URL Encoded	0.0	6	0.0	1879	0	6	1879	0
eXtensible Markup Language	0.3	318	0.6	375794	34	318	385190	35
Data	0.1	50	14.6	9120711	844	50	9135257	846
Compuserve GIF	0.0	37	0.1	52501	4	37	56063	5

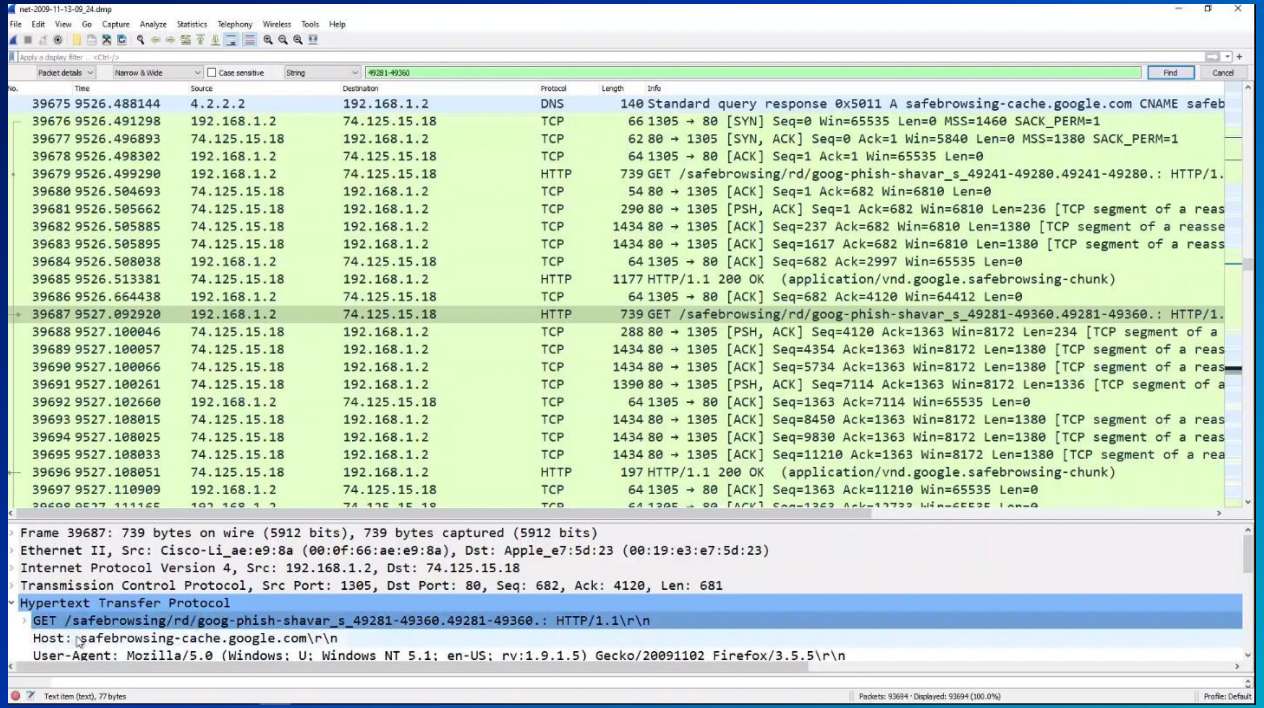
Display filters



HTTP request statistics

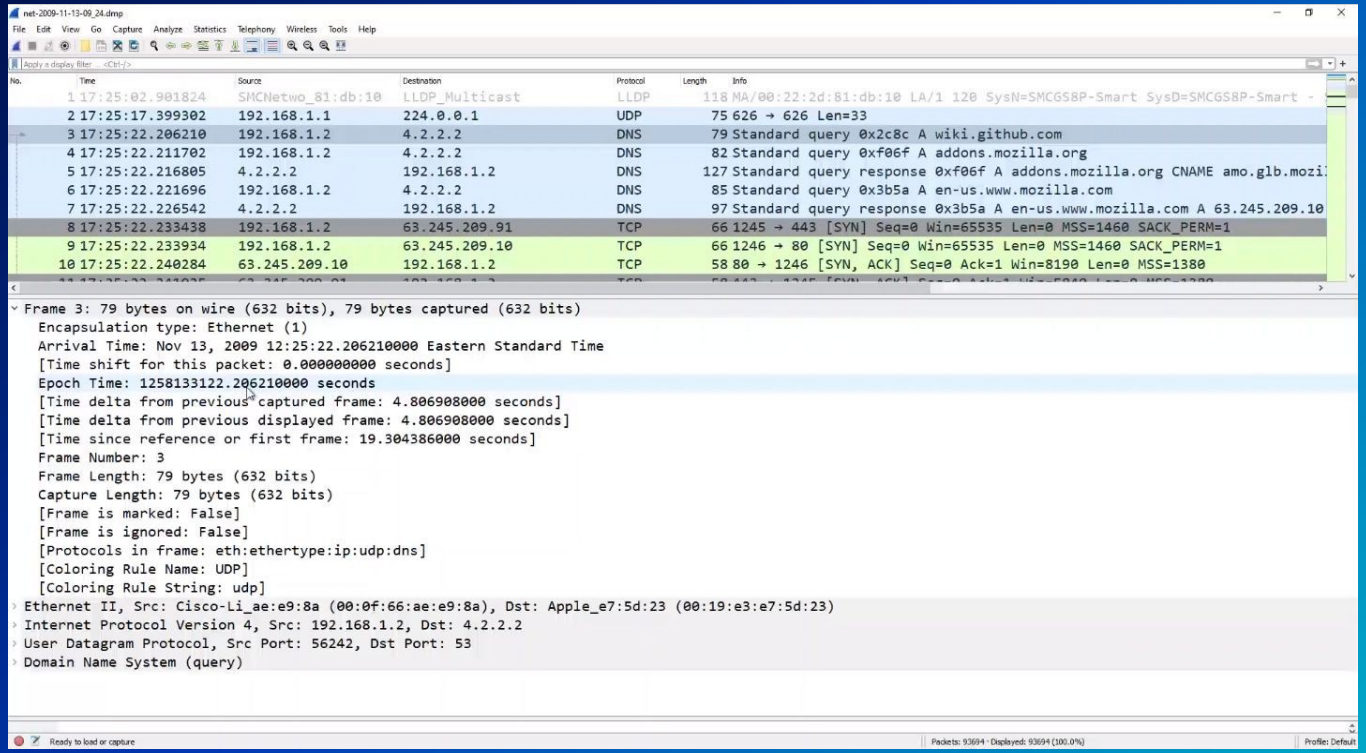


String searches

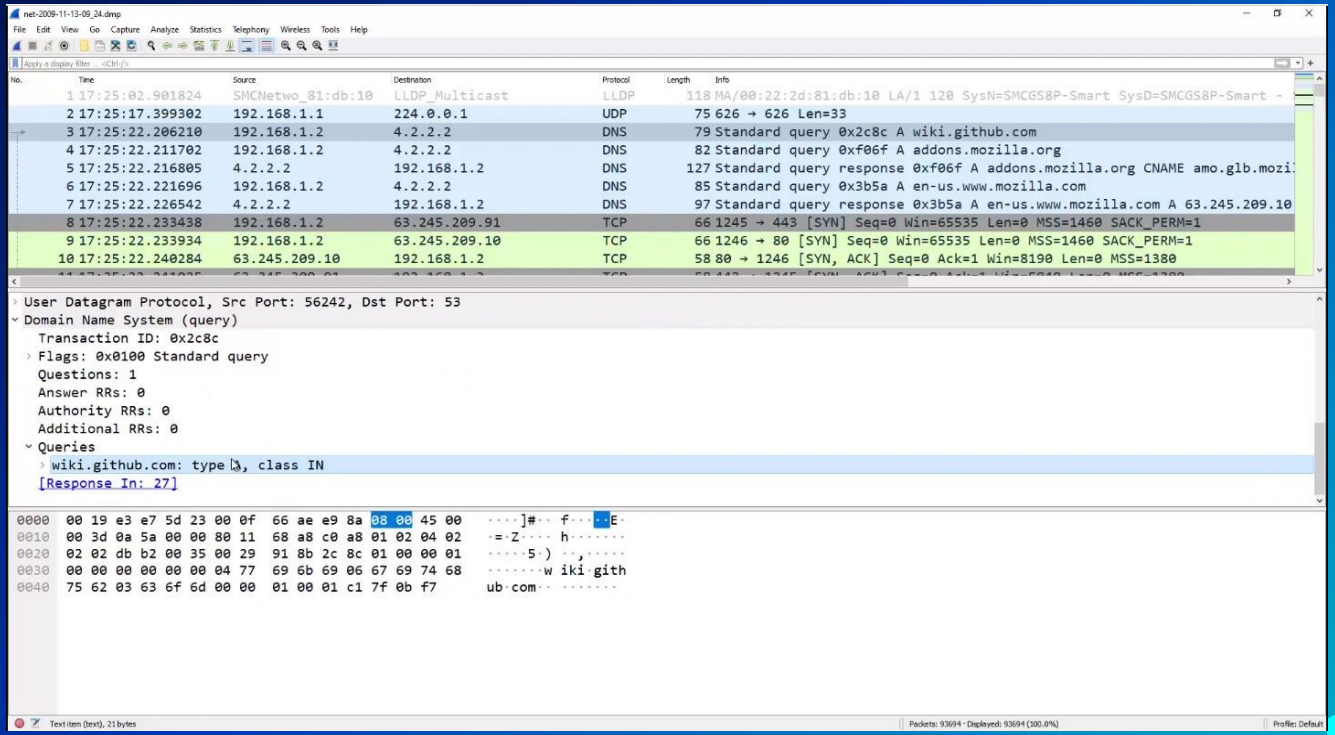


NetDef

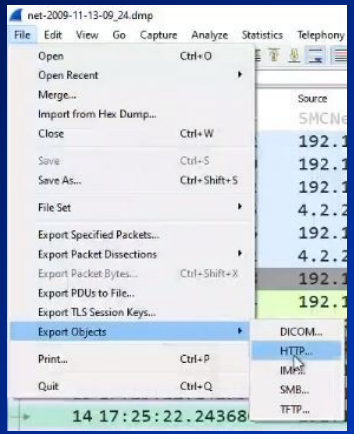
Time settings

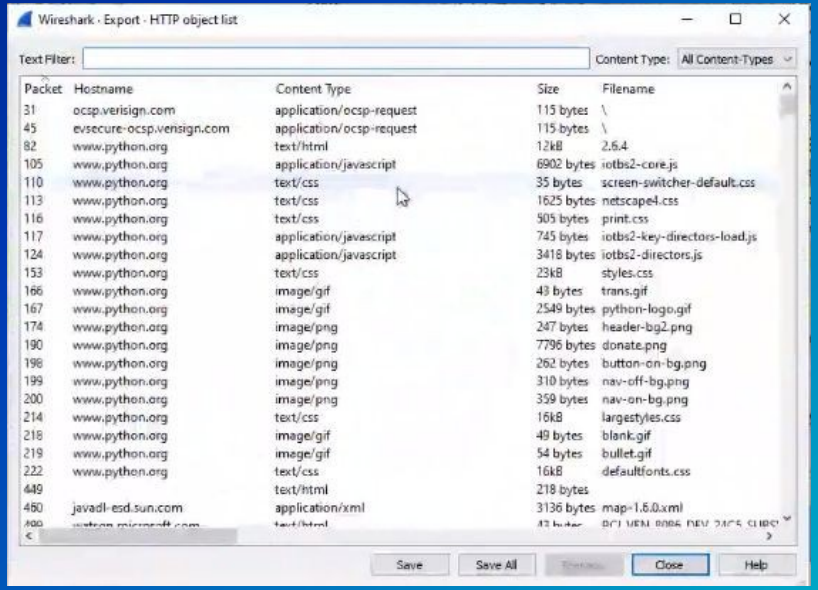


Packet details

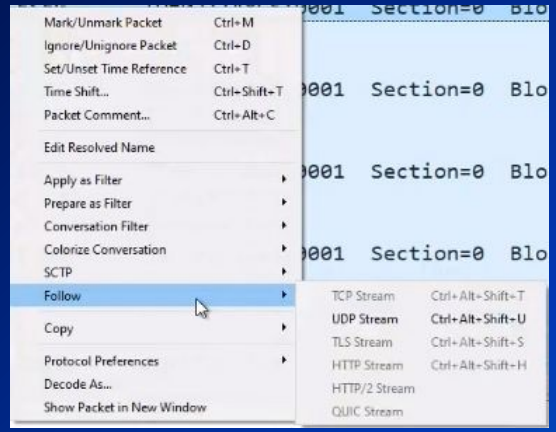


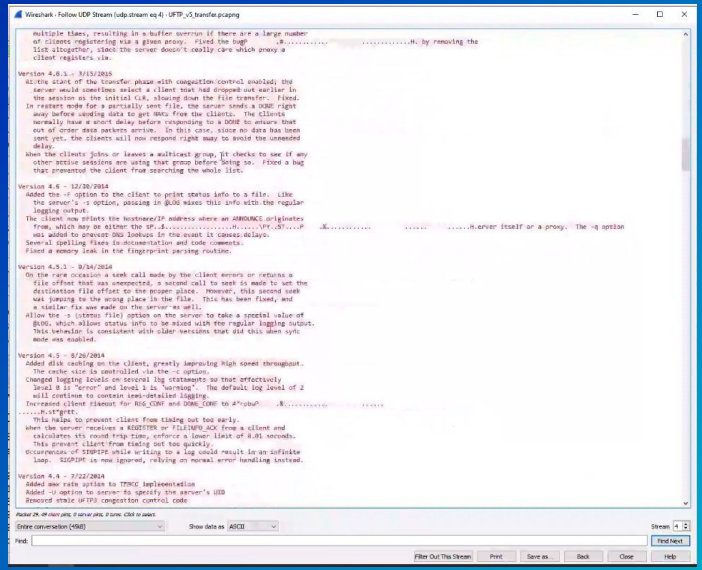
Export objects





Following packet streams





Guided Exercise: Capturing and Analyzing Packets

Steps:

- Open Wireshark
- Find the active network interface and double-click to start the capture
- Open a web browser and navigate to http://www.buffalony.gov/
  Close your browser and stop the packet capture
- Open the protocol hierarchy statistics window and note the protocols
- Filter the packet list to display HTTP traffic
- Run a string search for buffalony.gov
- Export HTTP objects and note the files that were transferred (hint: you may have to manually change the filename to a valid image file)

Summary

- Packets are powerful, but require infrastructure considerations to capture, store, and analyze
- Encrypted traffic can hinder the effectiveness of packet analysis activities
- Tools, like Wireshark, are instrumental in analyzing network traffic and identifying patterns of activity and data transmitted across a network

NetDef

Homework

- You have been provided with a PCAP (packet capture) file. Your job is to review the network traffic to identify the "flags" hidden throughout. There are 5 flags. For each flag you capture, provide the following information:
  - The flag itself
  - A brief description of the type of network traffic examined to identify the flag (e.g., protocol, source, destination) (1-2 sentences)
  - A screenshot of the captured flag (from Wireshark, or exported files from Wireshark
- Hints!
  - Remember the exercises today-- use the Wireshark functions you learned to find the flags!

NetDef

Homework

- Flag 1: Haveibeenpwned?
  - What is the email address of the user involved in this network activity?
- Flag 2: What's the password?
  - The user logs into a server (or servers) with a specific password, what is it?
- Flag 3: Switching things up...
  - The user tries to change the above password, but can't. Why not?
- Flag 4: Hidden in plain sight...
  - The user has accessed three files over FTP, but one in particular looks suspicious. What is the file?
- Flag 5: Higher-level thinking...
  - What are all of the protocols used throughout this PCAP? Of the identified protocols, document the security significance of at least one of them.

NetDef

Additional Resources

- Autopsy (Digital Forensics Platform and Graphical Interface)
  - https://www.autopsy.com/
- Wireshark Wiki - Sample Captures
  - https://wiki.wireshark.org/SampleCaptures
- Wireshark User's Guide (Advanced Topics = Chapter 7)
  - https://www.wireshark.org/docs/wsug_html/
- FTK Imager (Data Preview and Imaging Tool)
  - https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager#:~:text=FTK%C2%AE%20Imager%20is%20a,%C2%AE%20(FTK)%20is%20warranted.

NetDef

If you have any questions, please DM us on mattermost or come to Office Hours!

NetDef