CIS:3345 Intrusion to Investigation

Part II

Chavez | Turner | Ponce

User Story

On May 14, 2021, our team was alerted to an intrusion within our system, we as the digital forensics team, and we as the intrusion detection team, were requested to study the case, documented in the GitHub is our findings (Digital Forensics) and our solutions to prevent this from happening in the future (Intrusion Detection). The email was first sent to an employee on May 3rd, which was an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan. Due to the recent event we, as the IDS team, will be working with the digital forensics team, not only find the root of the problem but also come together and create a solution so that this will not happen again.

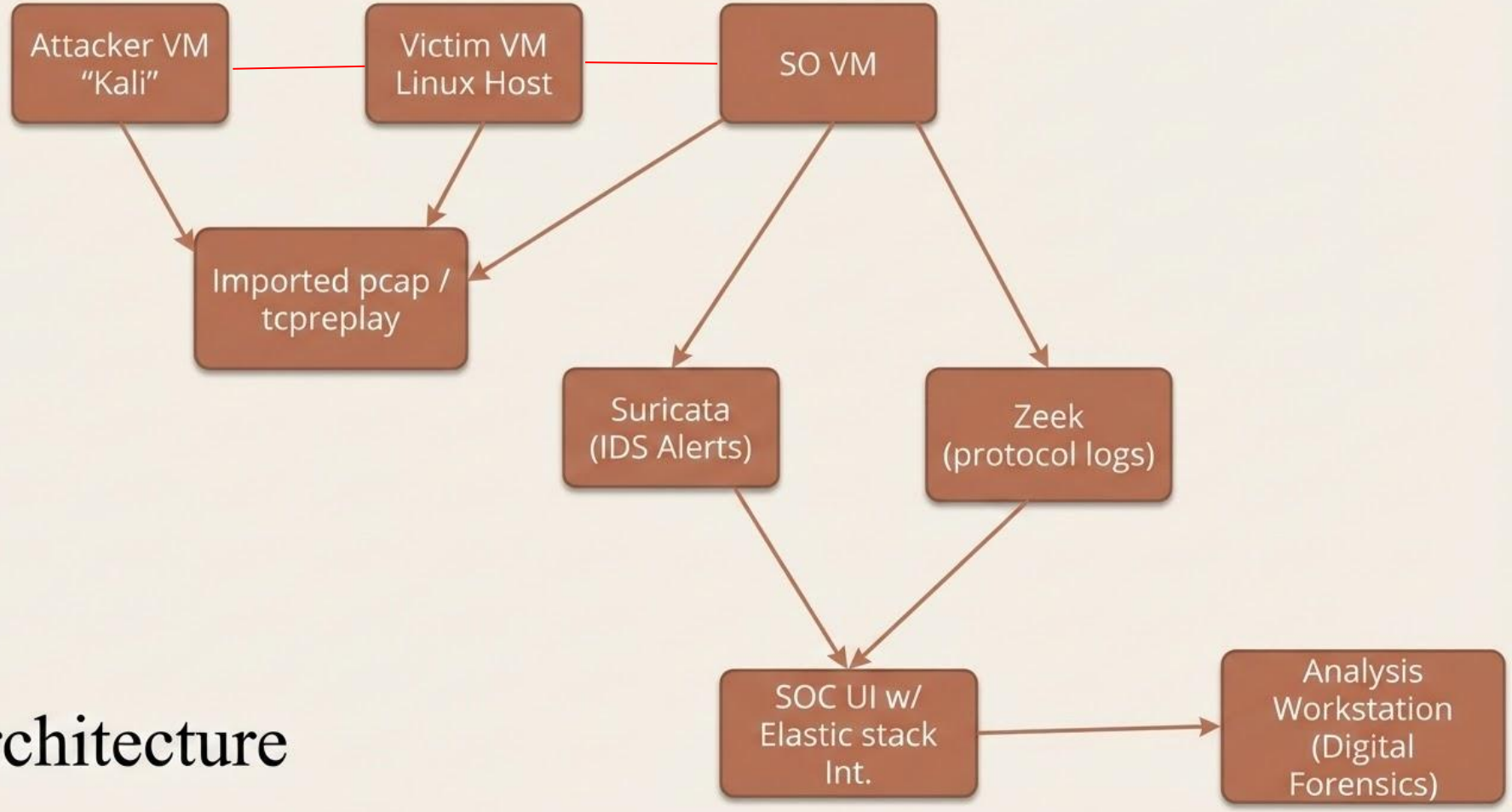
Summary of the Project

Our digital forensics project treats the provided pcap as real-world evidence from a suspected malware incident. We define the case scope, document chain-of-custody, and hash the evidence to show it hasn’t been altered. Using Wireshark, we reconstruct the attack timeline and extract key artifacts like malicious IPs, domains, and payloads. Finally, we turn those findings into a concise case report with an IOC list and practical recommendations that a blue team could actually deploy.

Materials

- A system with Wireshark
- VMware
- Security Onion
- Kali system run through the VM
- https://www.malware-traffic-analysis.net/index.html
- Private network, to be able to utilize security onion and its resources without anything blocking or interfering

Architecture

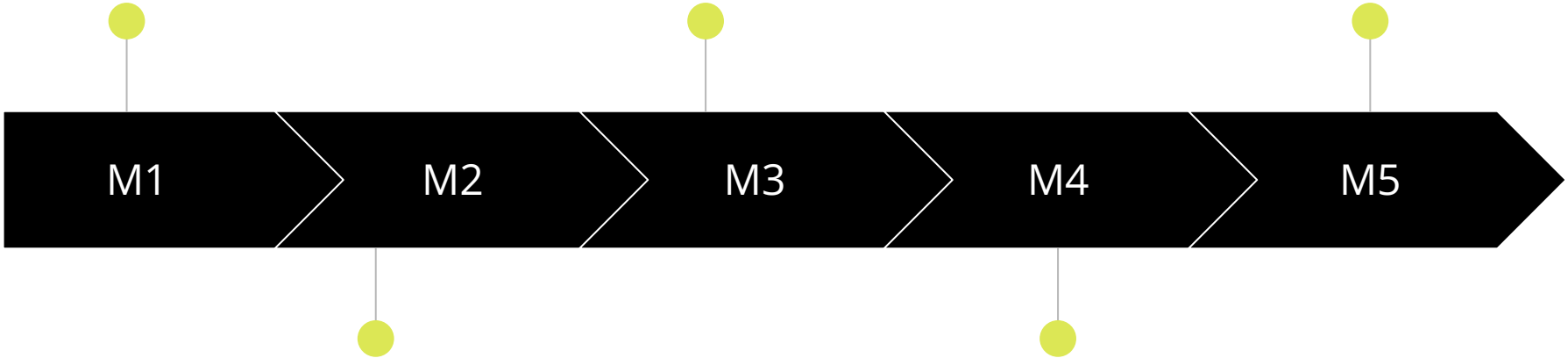


MILESTONES

Case scope, chain-of-custody.

(Optional) Memory/Disk triage and correlation to PCAP.

Future work

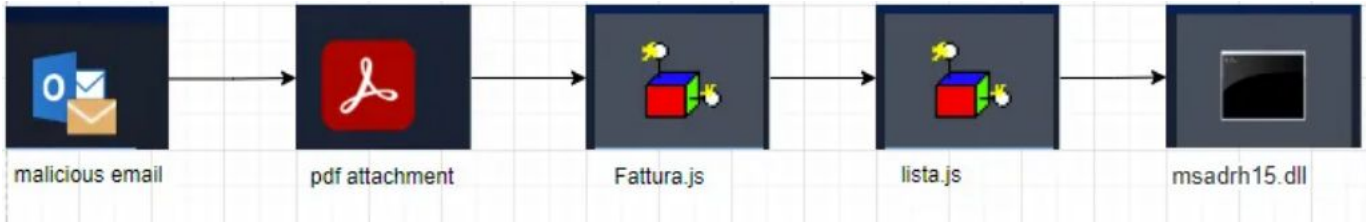


Wireshark reconstruction + artifact extraction.

Final case report + IOC list + recommendations + demo.

Initial Attack

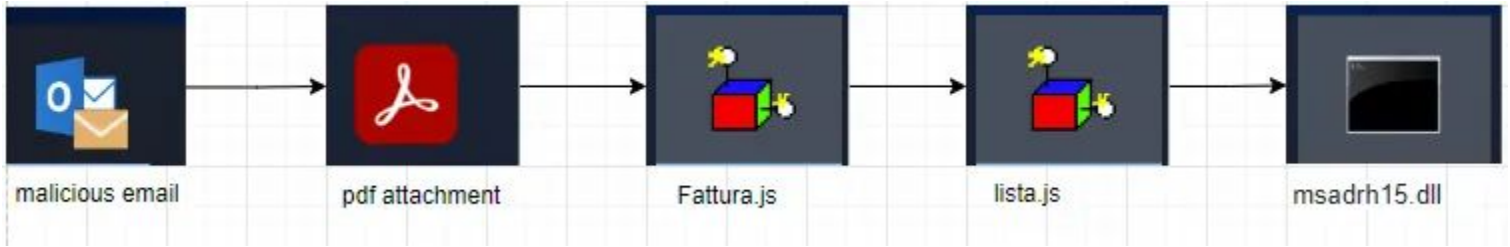
The email was first sent to an employee on May 3rd, which was an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan. Trojan Path is as follows:



Ursnif, the banking trojan

Ursnif is a variant of the GOZI malware, usually disguises itself as a part of an invoice, was first seen in 2006, but had its script leaked in 2015, making it more accessible to other. So now it has a github:

- https://github.com/MBCProject/mbc-markdown/blob/main/xample-malware/ursnif.md



Milestone 1 - Case scope, chain-of-custody, evidence hashing.

- Brief overview of the case
- Identify evidence
- Chain of Custody
- Scope

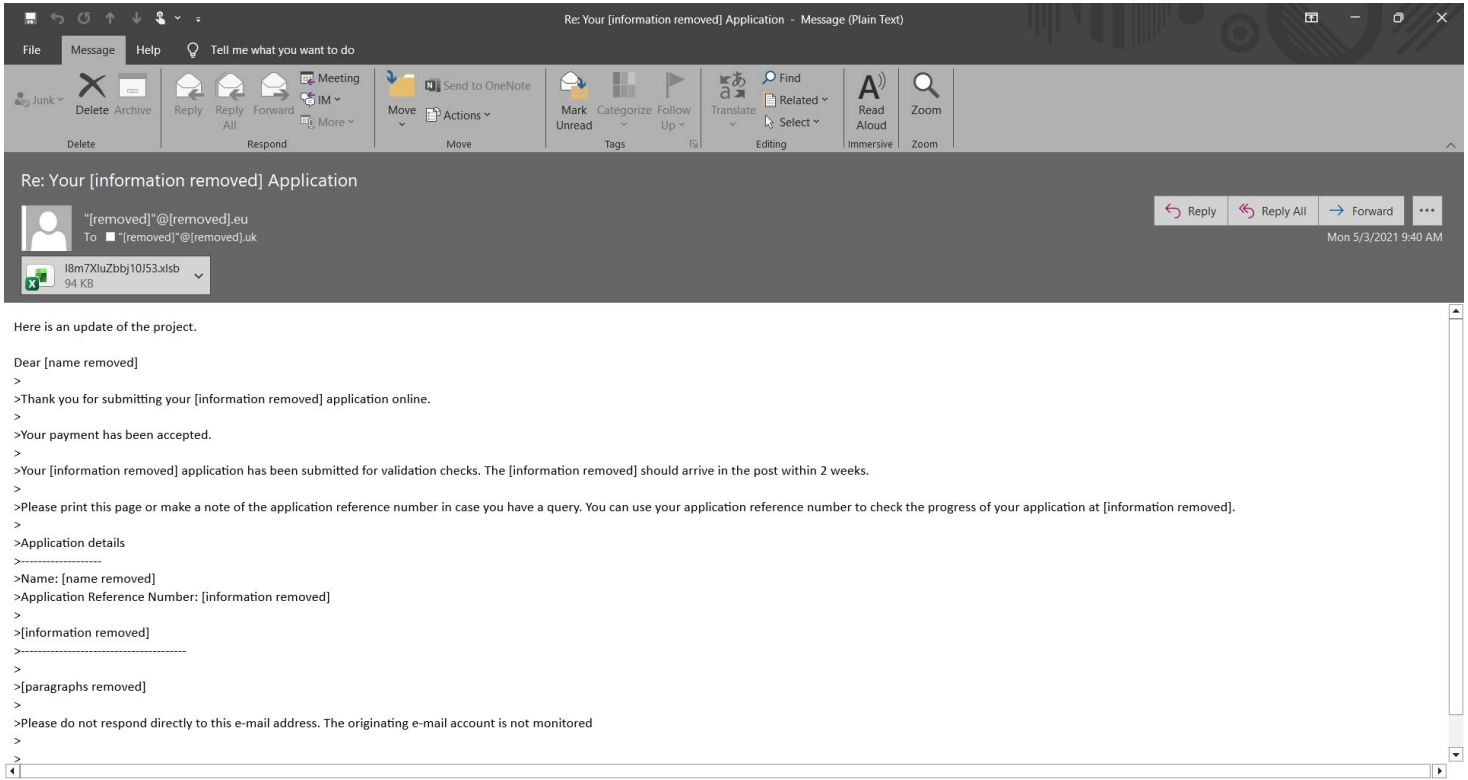
CASE FILE:

First documented on May 3rd a suspicious email was sent to an employee, this email contained an excel sheet with the macros for URSNIF. On May 14th another email was sent, that was similar in nature. URSNIF is more commonly referred to as a banking trojan. Originally identified in 2006, there was a GitHub leak of the source code for this trojan.

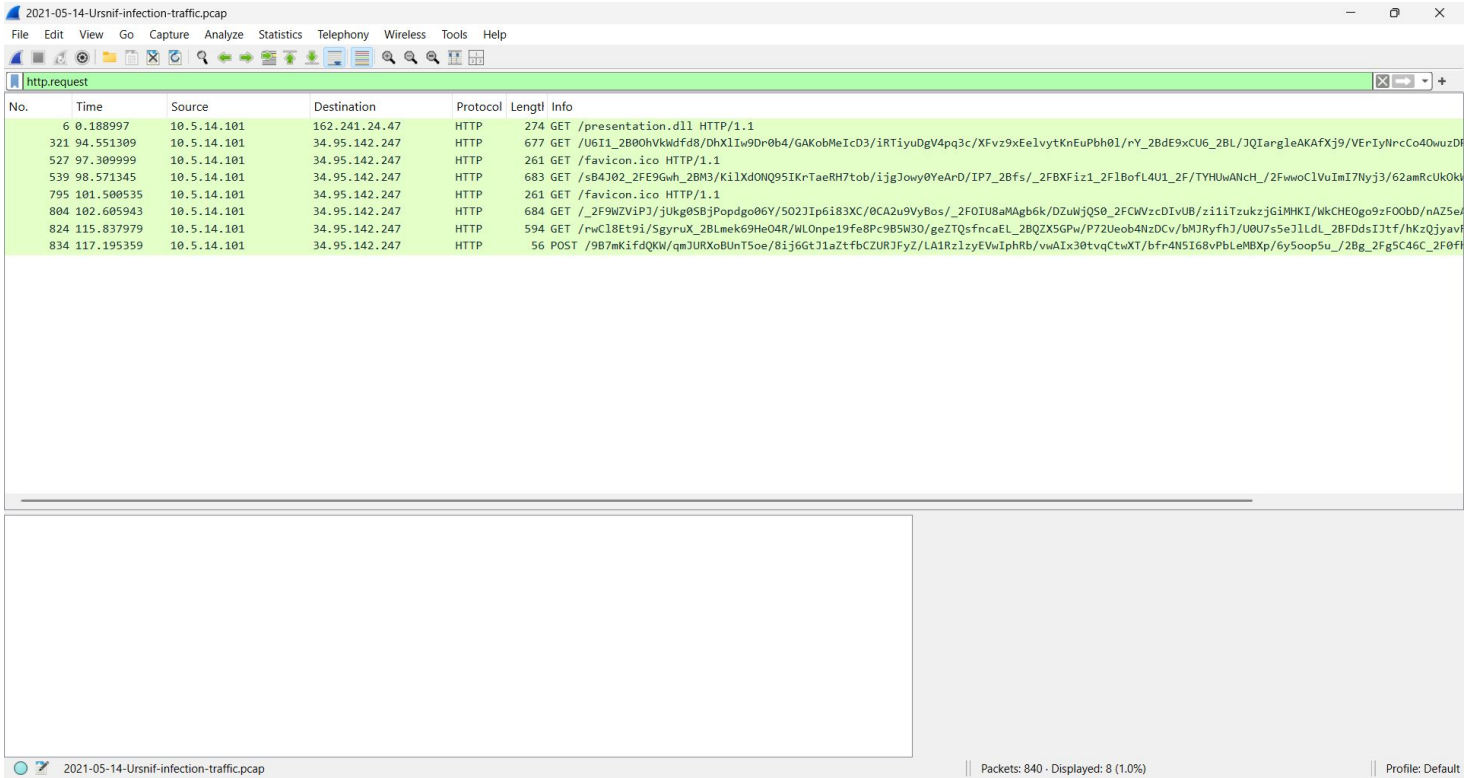
Evidence on hand

- Original Email file sent, See Figure 1.
- Pcaps that were sent, See Figure 2.
- Excel sheet attached, See Figure 3.

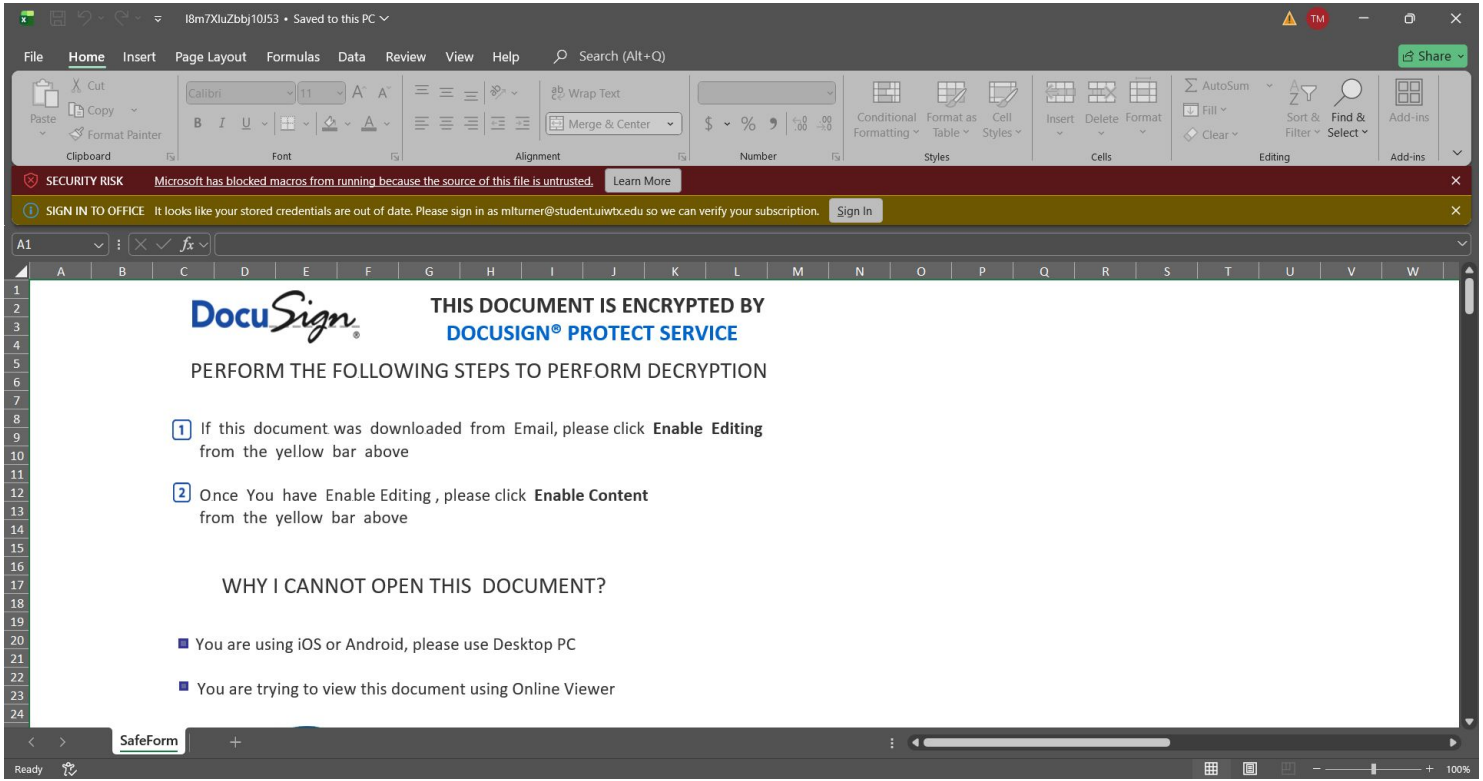
Original Phishing email (Figure 1)



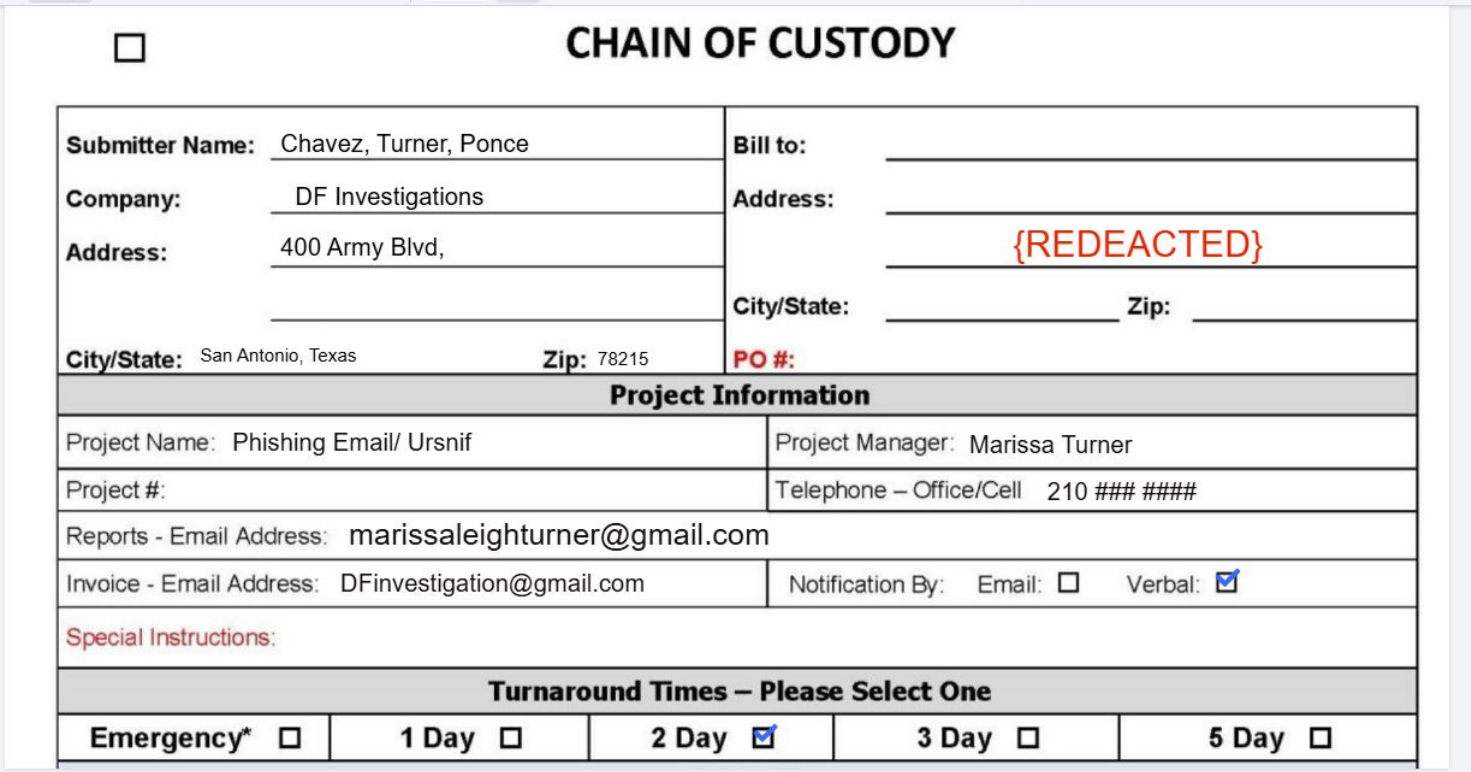
Wireshark Analysis of Pcap file (Figure 2)



Excel Sheet (Figure 3)



Chain of Custody Chart



CHAIN OF CUSTODY

Submitter Name: Chavez, Turner, Ponce	**Bill to:**
Company: DF Investigations	**Address:**
Address: 400 Army Blvd,	{REDEACTED}
	City/State: **Zip:**
City/State: San Antonio, Texas **Zip:** 78215	**PO #:**

Project Information

Project Name: Phishing Email/ Ursnif	Project Manager: Marissa Turner
Project #:	Telephone – Office/Cell 210 ### ####
Reports - Email Address: marissaleighturner@gmail.com	
Invoice - Email Address: DFinvestigation@gmail.com	Notification By: Email: ☐ Verbal: ☑
Special Instructions:	

Turnaround Times – Please Select One

Emergency* ☐	**1 Day** ☐	**2 Day** ☑	**3 Day** ☐	**5 Day** ☐

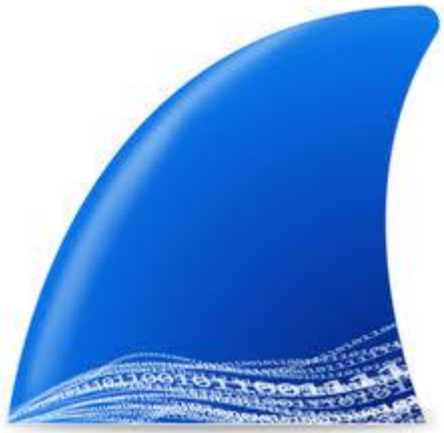
Scope

This project designs, implements, and documents an end-to-end workflow that uses Security Onion (Suricata + Zeek) and Wireshark-based digital forensics to detect, reconstruct, and analyze a malware infection in captured network traffic, then produce actionable IOCs, a case report, and a short live demo that shows how detection and investigation work together.

Milestone 2 - Wireshark Reconstruction & Artifact Extraction

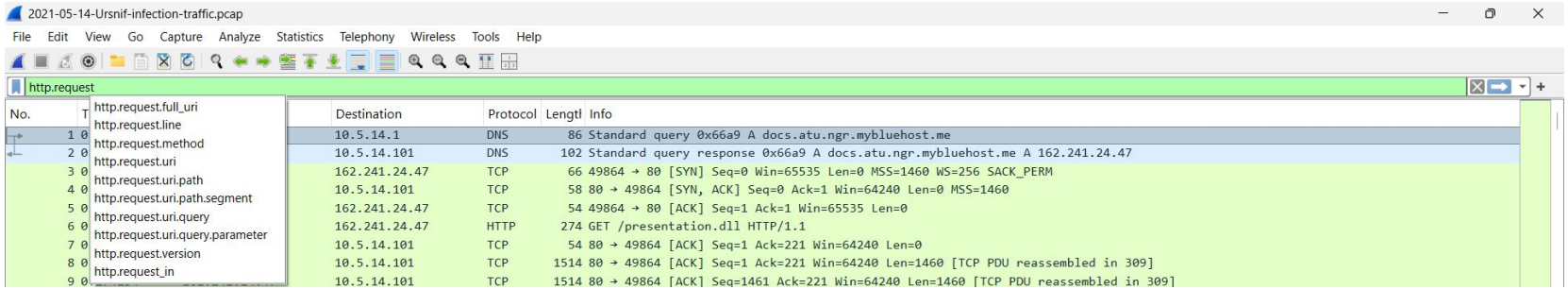
- Configure Wireshark
- Pass Malicious PCAPs
- Draw connections between entries

M2 - Wireshark Reconstruction



- Disabling noisy traffic
- Customizing columns
- TCP sream

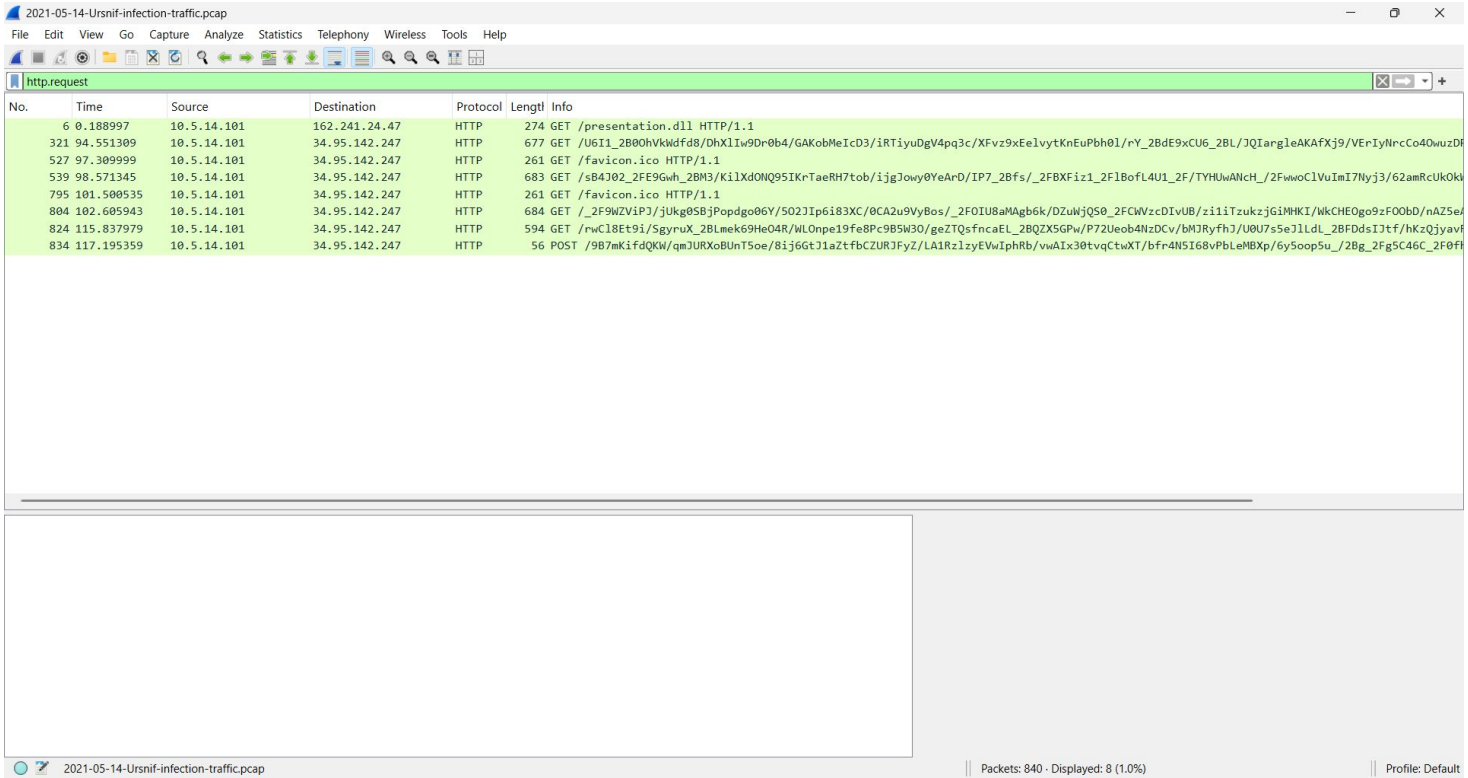
CUSTOM FILTERS



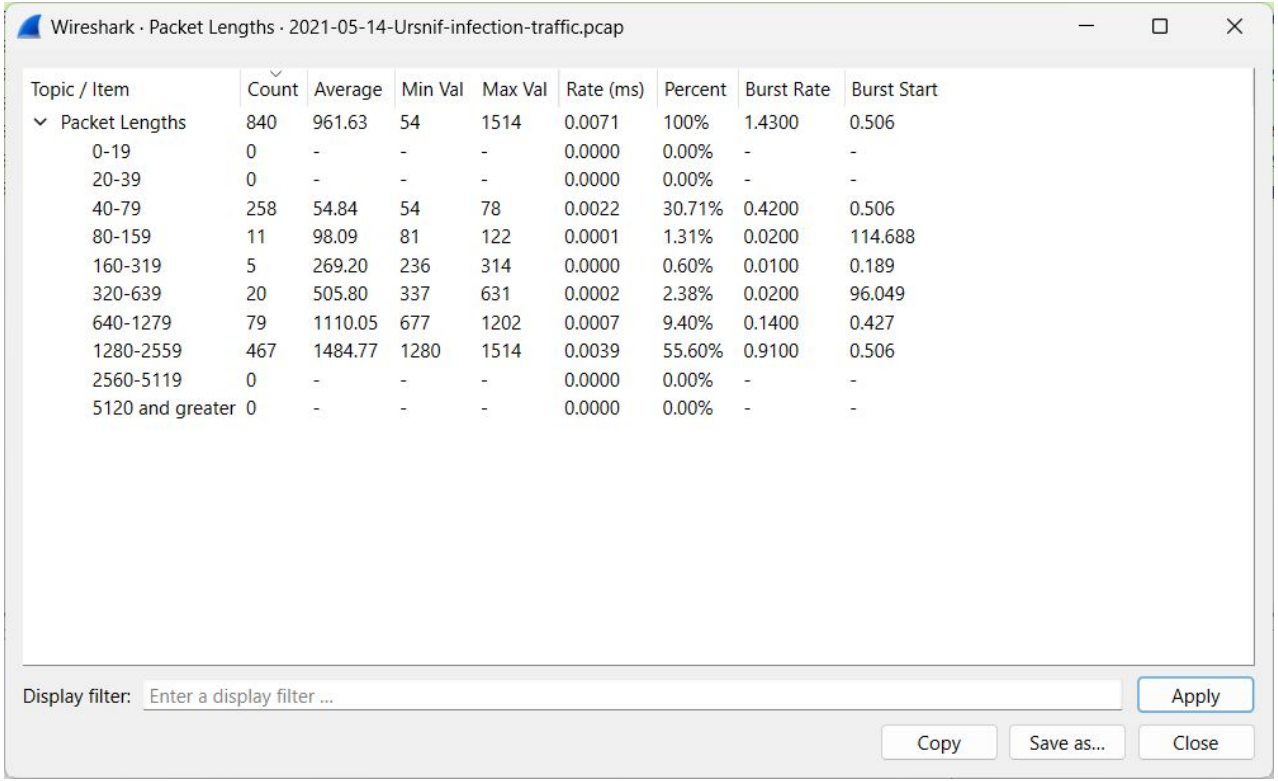
M2 – Malware PCAPs

- Extract the PCAP evidence
- Identify Top Talkers & Key Protocols
- Marked suspicious IP addresses

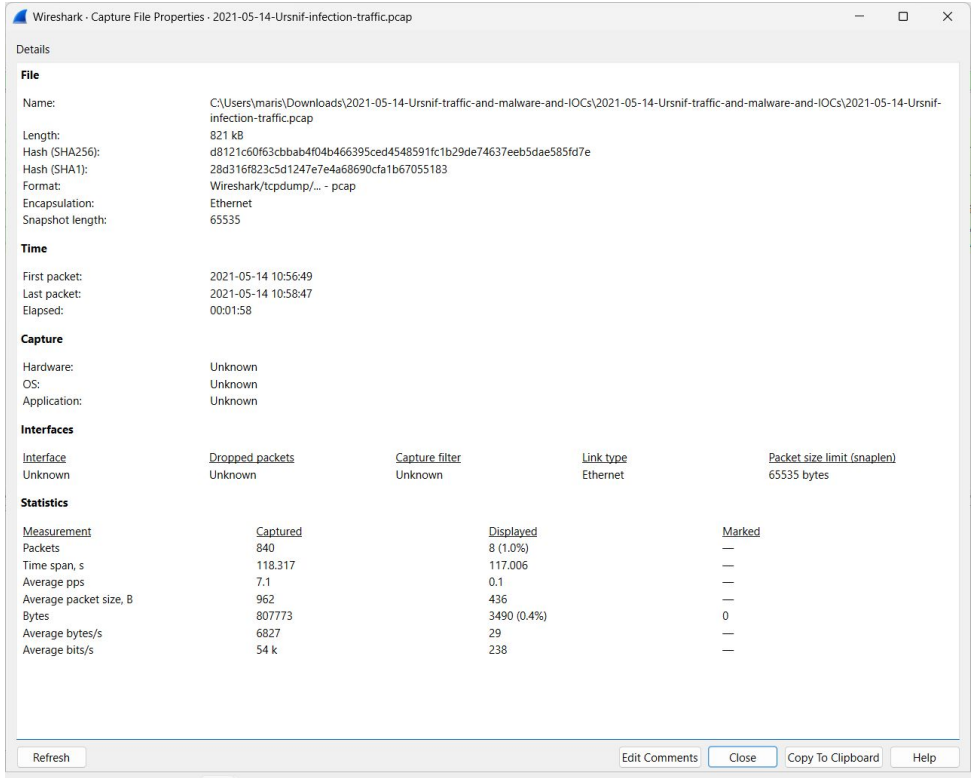
Wireshark Analysis of Pcap file



Wireshark Analysis of Pcap File



Wireshark Statistics (Filtered)



Milestone 4 – Final Case Report IOC list recommendations demo

- IOC List
- Practical Recommendations

M4 – IOC list

- Email IOCs
- File IOCs

M4 – Practical Recommendations

- Strengthen web and email defenses
- Harden endpoints and browsers
- Improve logging, monitoring, and IOC use
- Policies, training, and response

Key Takeaways

- Treated PCAP as real evidence
  - Case scope, chain of custody
- Wireshark Reconstruction
- Extracted concrete artifacts
- Findings directly tied with IDS side

GITHUB

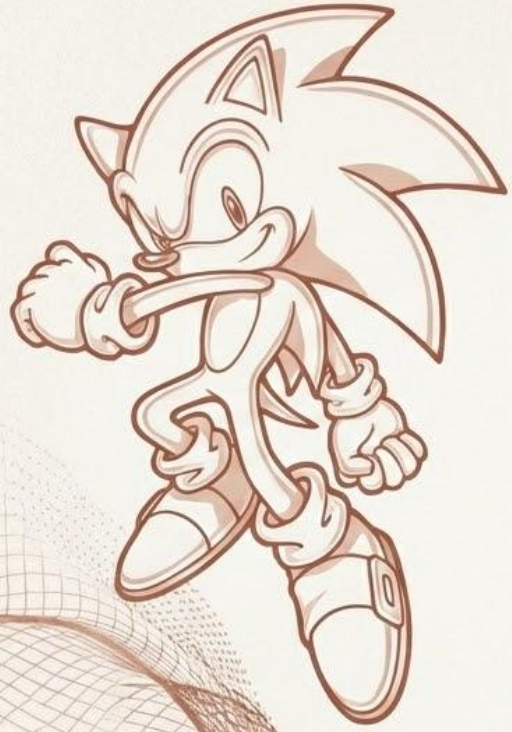
https://github.com/mwchavez/IDS_DF_F2025_Project_MC_MT_DP

Future Status of the project

- Expand evidence sources
- Automate IOC extraction

Resources used in gathering information

- https://www.malware-traffic-analysis.net/2021/05/14/index.html
- https://github.com/MBCProject/mbc-markdown/blob/main/xample-malware/ursnif.md
- https://www.acronis.com/en/tru/posts/ursnif-the-banking-trojan/
- https://attack.mitre.org/software/S0386/



Thank You!!