

# CIS:3345

## Intrusion to Investigation

### Part II

Chavez | Turner | Ponce



# User Story

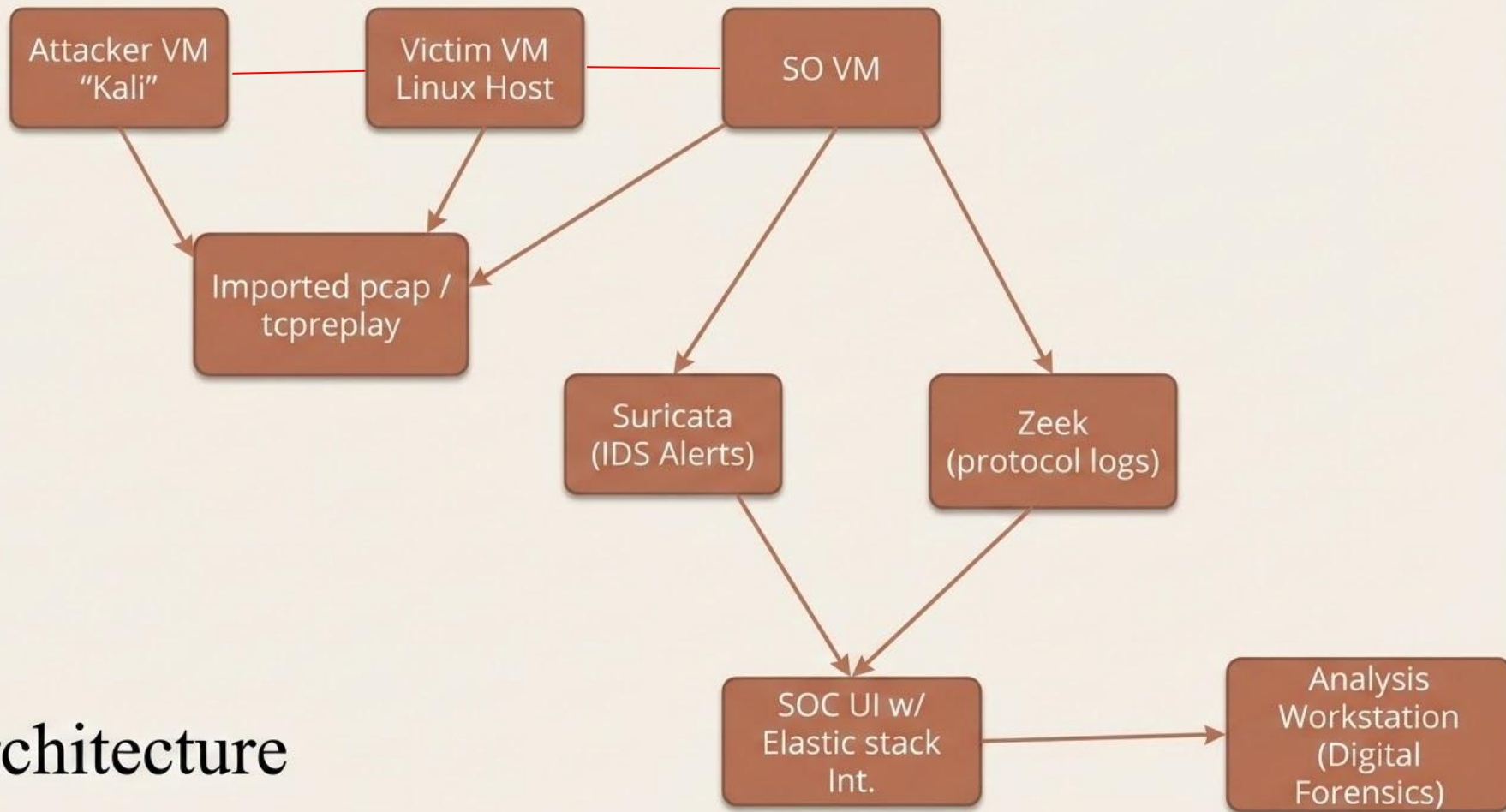
On May 14, 2021, our team was alerted to an intrusion within our system, we as the digital forensics team, and we as the intrusion detection team, were requested to study the case, documented in the GitHub is our findings (Digital Forensics) and our solutions to prevent this from happening in the future (Intrusion Detection). The email was first sent to an employee on May 3<sup>rd</sup>, which was an excel sheet with the macros for URSNIF. On May 14<sup>th</sup> 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



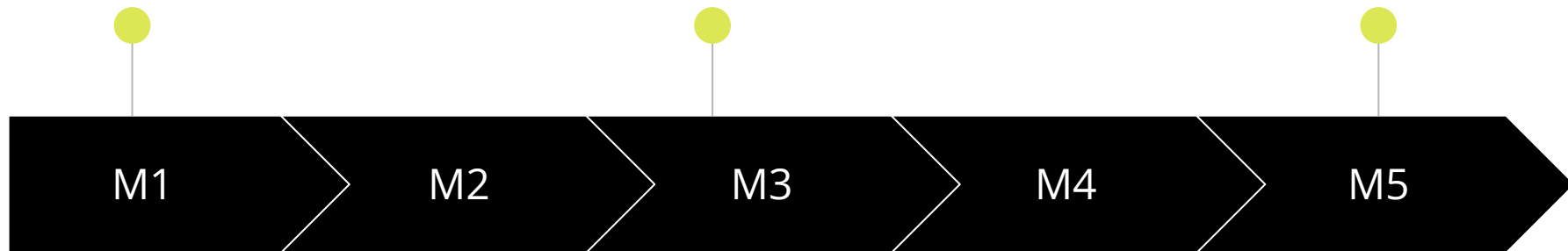
# MILESTONES



Case scope,  
chain-of-custody.

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

Future work

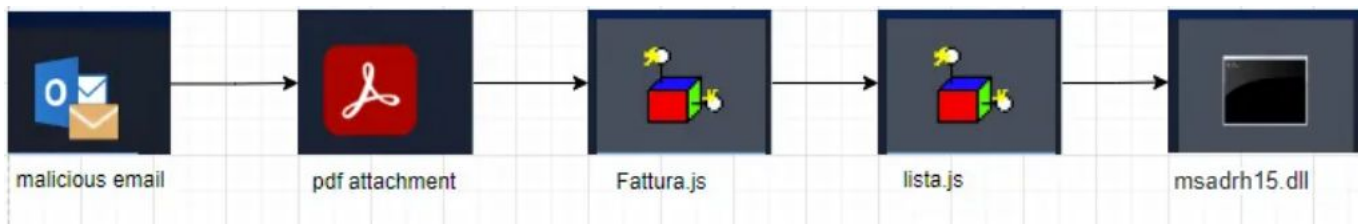


Wireshark  
reconstruction +  
artifact extraction.

Final case report + IOC  
list + recommendations +  
demo.

# Initial Attack

The email was first sent to an employee on May 3<sup>rd</sup>, which was an excel sheet with the macros for URSNIF. On May 14<sup>th</sup> 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:

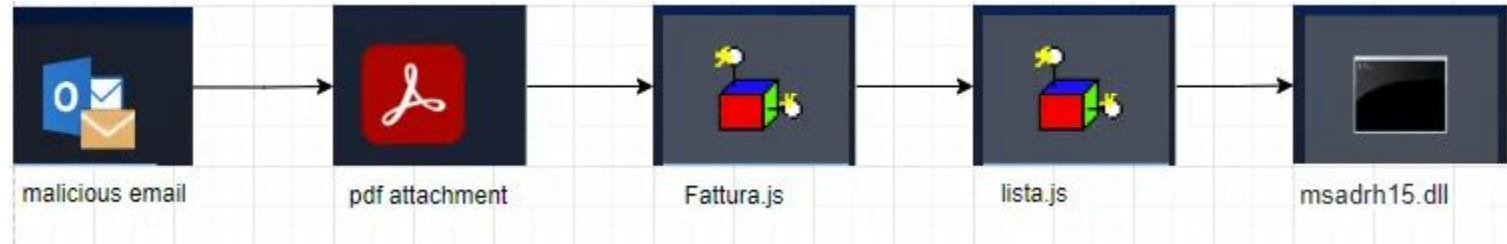




# Ursnif, the banking trojan

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
-

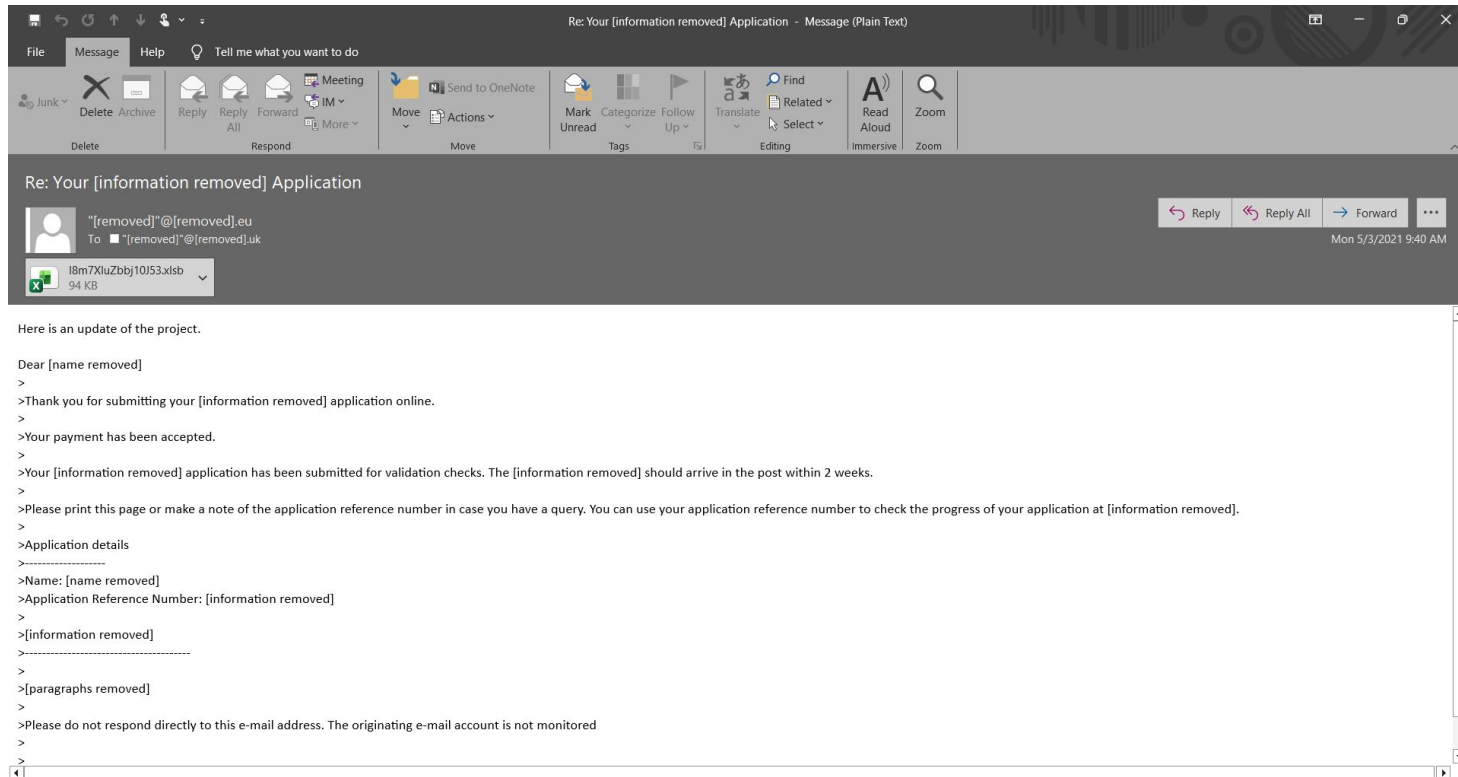
# CASE FILE:

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 14<sup>th</sup> 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.

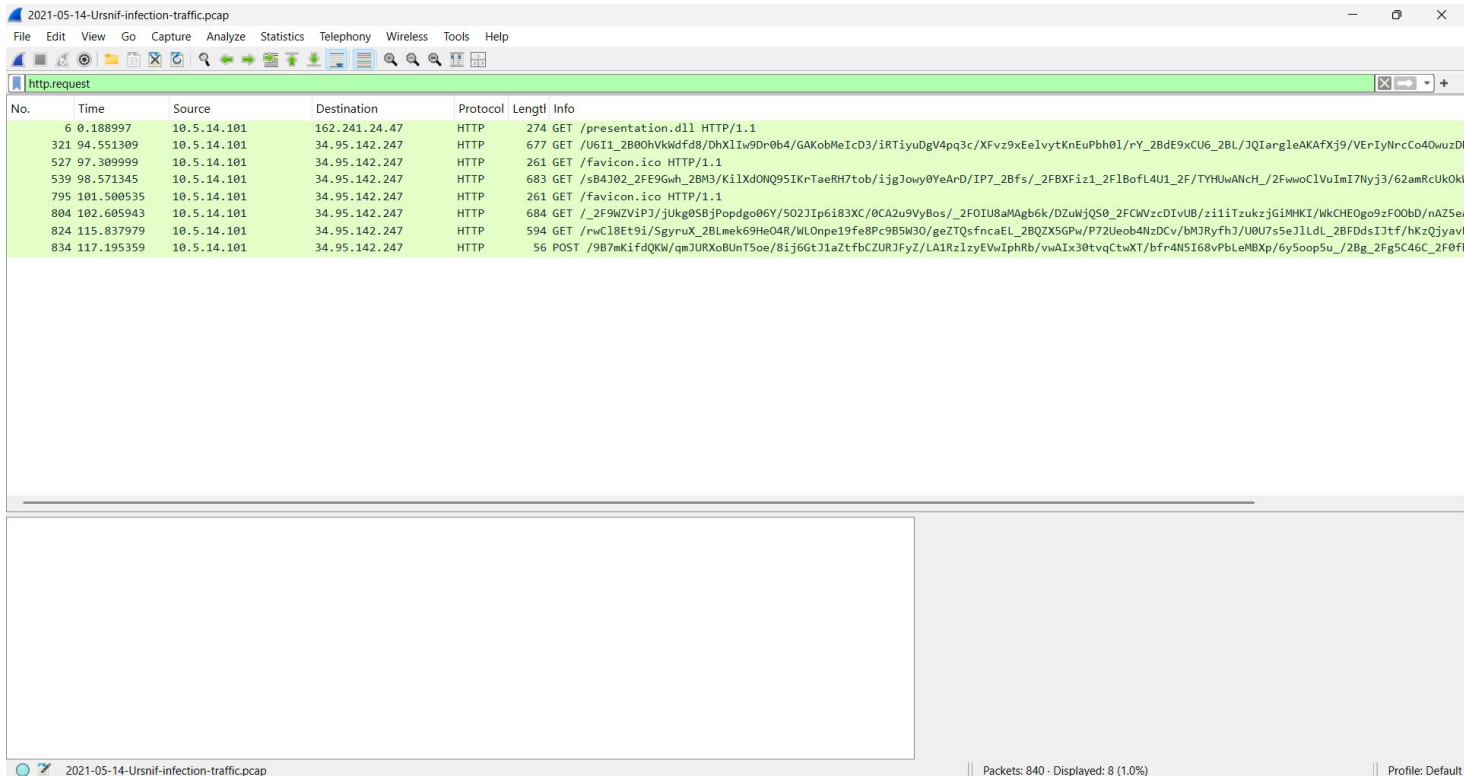
# Evidence on hand

- 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)



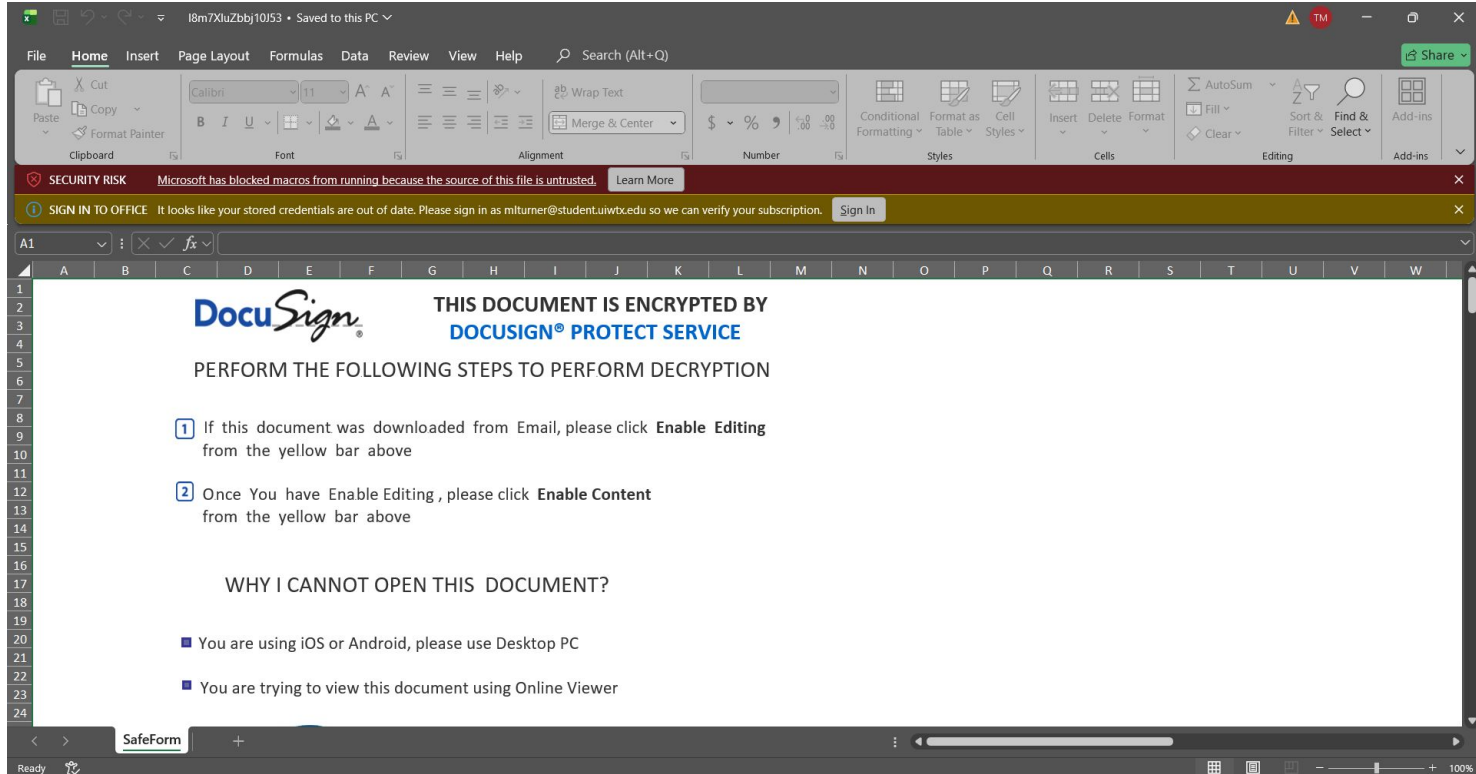
The image shows the Wireshark network protocol analyzer interface. The title bar indicates the file being analyzed is "2021-05-14-Ursnif-infection-traffic.pcap". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The main display area shows a list of captured packets, with the first packet selected and its details expanded to show an HTTP request.

The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
6	0.188997	10.5.14.101	162.241.24.47	HTTP	274	GET /presentation.dll HTTP/1.1
321	94.551309	10.5.14.101	34.95.142.247	HTTP	677	GET /U6I1_2B80hVkkidf8/DhXLIw9Dr0b4/GAKobMeICD3/iRTiyuDgV4pq3c/XFvz9xE1vytKnEuPbh01/rY_2BdE9xCU6_2BL/JQIarg1eAKAFXj9/VErIyNrcCo40wuzDF
527	97.309999	10.5.14.101	34.95.142.247	HTTP	261	GET /favicon.ico HTTP/1.1
539	98.571345	10.5.14.101	34.95.142.247	HTTP	683	GET /sB4J02_2FE9Gwh_2BM3/K1lXdONQ95IKrTaeRH7tob/ijgJowy0YeArD/IP7_2Bfs/_2FBXFiz1_2F1BoFl4U1_2F/TYHUwANcH/_2FwwoC1VuImI7Nyj3/62amRcUkOkk
795	101.500535	10.5.14.101	34.95.142.247	HTTP	261	GET /favicon.ico HTTP/1.1
804	102.605943	10.5.14.101	34.95.142.247	HTTP	684	GET /_2F9WZV1Pj/jUkg0SBJPopdgo06Y/502J1p6i83XC/0CA2u9VyBos/_2FOIu8aMAgb6k/DZukjQ50_2FCWVzcDIvUB/z1i1TzukzjGiMhKI/wkCHE0go9zFOObD/nAZ5e
824	115.837979	10.5.14.101	34.95.142.247	HTTP	594	GET /rwC18Et9i/SgyruX_2BLmek69He04R/WLOnpe19fe8Pc9B5W30/geZTQsfncEL_2BQZX5GPw/P72Ueob4NzDCv/bMJRyfhj/U0U7s5eJlIdL_2BFDdsI3tf/hKzQjyavf
834	117.195359	10.5.14.101	34.95.142.247	HTTP	56	POST /9B7mKifdQKW/qmJURXoBUnT5oe/8ij6GtJ1aZtfbCZURJFyZ/LA1Rz1zyEVwIphRb/vwAIx30tvqCtwXT/bFr4N5I68vPbLEMBXp/6ySooP5u/_2Bg_2Fg5C46C_2F0Ff

The status bar at the bottom shows "2021-05-14-Ursnif-infection-traffic.pcap" on the left, "Packets: 840 · Displayed: 8 (1.0%)" in the center, and "Profile: Default" on the right.

# Excel Sheet (Figure 3)



# Chain of Custody Chart

<input type="checkbox"/> CHAIN OF CUSTODY				
<b>Submitter Name:</b> Chavez, Turner, Ponce		<b>Bill to:</b> _____		
<b>Company:</b> DF Investigations		<b>Address:</b> _____		
<b>Address:</b> 400 Army Blvd,		_____ {REDEACTED}		
_____		<b>City/State:</b> _____ <b>Zip:</b> _____		
<b>City/State:</b> San Antonio, Texas		<b>PO #:</b> _____		
<b>Project Information</b>				
Project Name: Phishing Email/ Ursnif		Project Manager: Marissa Turner		
Project #:		Telephone – Office/Cell 210 ### ####		
Reports - Email Address: marissaleightturner@gmail.com				
Invoice - Email Address: DFInvestigation@gmail.com		Notification By: Email: <input type="checkbox"/> Verbal: <input checked="" type="checkbox"/>		
<b>Special Instructions:</b>				
<b>Turnaround Times – Please Select One</b>				
<b>Emergency*</b> <input type="checkbox"/>	<b>1 Day</b> <input type="checkbox"/>	<b>2 Day</b> <input checked="" type="checkbox"/>	<b>3 Day</b> <input type="checkbox"/>	<b>5 Day</b> <input type="checkbox"/>



# 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 stream

---

# CUSTOM FILTERS

2021-05-14-Ursnif-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

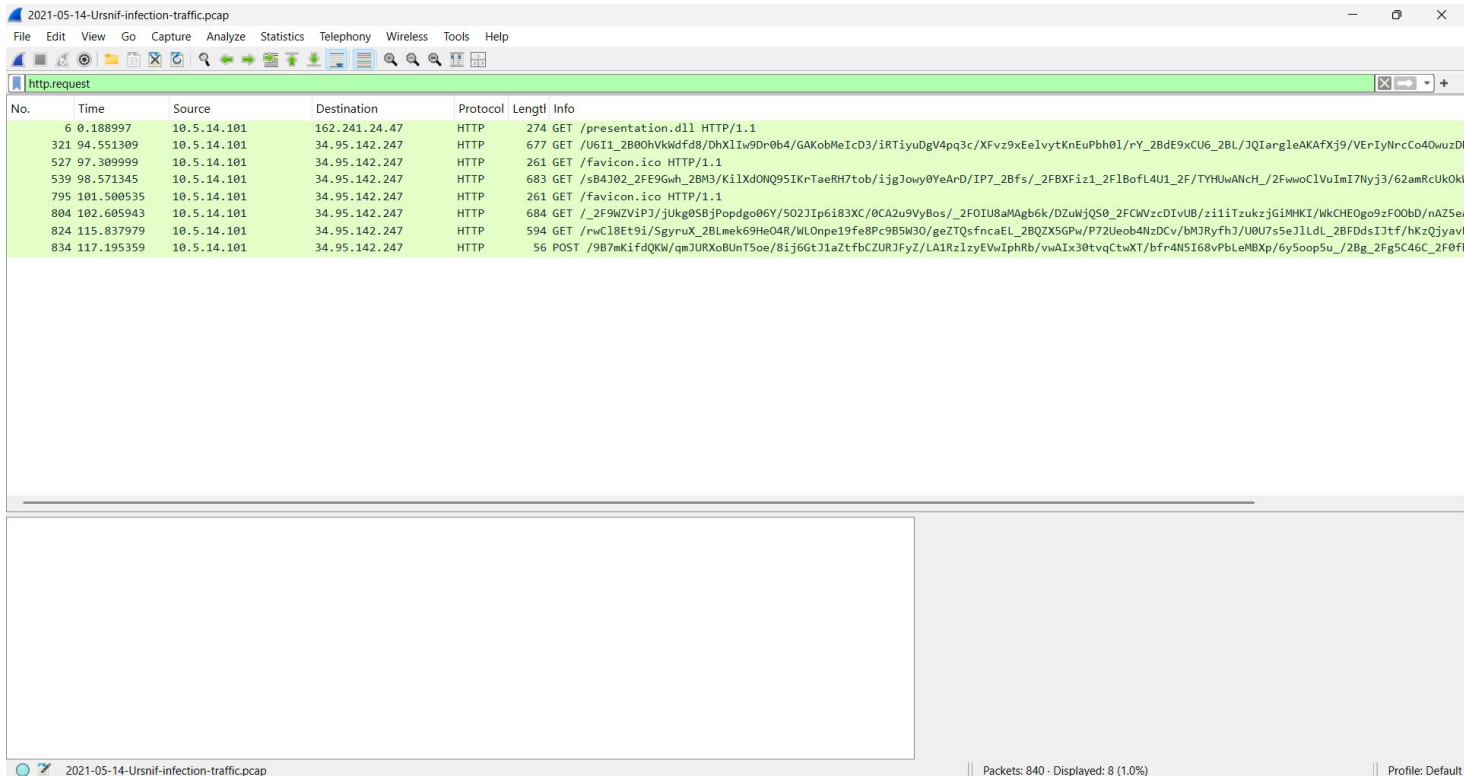
No.	Destination	Protocol	Length	Info
1 0	10.5.14.1	DNS	86	Standard query 0x66a9 A docs.atu.ngr.mybluehost.me
2 0	10.5.14.101	DNS	102	Standard query response 0x66a9 A docs.atu.ngr.mybluehost.me A 162.241.24.47
3 0	162.241.24.47	TCP	66	49864 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
4 0	10.5.14.101	TCP	58	80 → 49864 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5 0	162.241.24.47	TCP	54	49864 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
6 0	162.241.24.47	HTTP	274	GET /presentation.dll HTTP/1.1
7 0	10.5.14.101	TCP	54	80 → 49864 [ACK] Seq=1 Ack=221 Win=64240 Len=0
8 0	10.5.14.101	TCP	1514	80 → 49864 [ACK] Seq=1 Ack=221 Win=64240 Len=1460 [TCP PDU reassembled in 309]
9 0	10.5.14.101	TCP	1514	80 → 49864 [ACK] Seq=1461 Ack=221 Win=64240 Len=1460 [TCP PDU reassembled in 309]

# M2 – Malware PCAPs



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

# Wireshark Analysis of Pcap file



2021-05-14-Ursnif-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

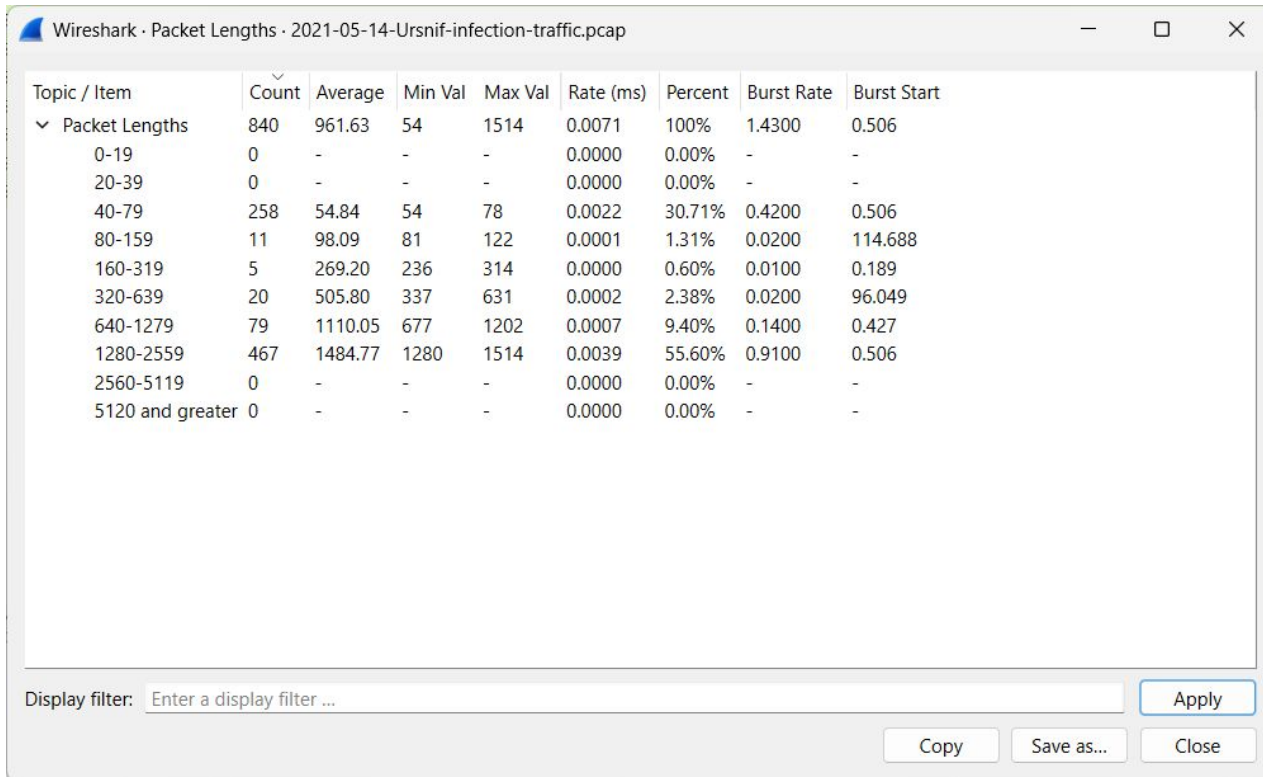
No.	Time	Source	Destination	Protocol	Length	Info
6	0.188997	10.5.14.101	162.241.24.47	HTTP	274	GET /presentation.dll HTTP/1.1
321	94.551309	10.5.14.101	34.95.142.247	HTTP	677	GET /U6I1_2B00hVkkidf8/DhXLIw9Dr0b4/GAKobMeIcD3/iRTiyuDgV4pq3c/XFvz9xE1vytKnEuPbh01/rY_2BdE9xCU6_2BL/JQIarg1eAKaFXj9/VErIyNrcCo40wuzDf...
527	97.309999	10.5.14.101	34.95.142.247	HTTP	261	GET /favicon.ico HTTP/1.1
539	98.571345	10.5.14.101	34.95.142.247	HTTP	683	GET /sB4J02_2FE9Gwh_2BM3/K1lXdONQ95IKrTaeRH7tob/ijgJowy0YeArD/IP7_2Bfs/_2FBXFiz1_2F1BoFL4U1_2F/TYHUwANcH/_2FwwoC1VuImI7Nyj3/62amRcUkOk...
795	101.500535	10.5.14.101	34.95.142.247	HTTP	261	GET /favicon.ico HTTP/1.1
804	102.605943	10.5.14.101	34.95.142.247	HTTP	684	GET /_2F9WZV1Pj/jUkg0SBJPopdgo06Y/502J1p6i83XC/0CA2u9VyBos/_2FOIu8aMAgb6k/DZukjQ50_2FCWVzcDIvUB/z1i1TzukzjGiMHKI/wkCHE0go9zFOObD/nAZ5e...
824	115.837979	10.5.14.101	34.95.142.247	HTTP	594	GET /rwC18Et9i/SgyruX_2Blmek69He04R/WLONpe19fe8Pc9B5W30/geZTQsfncaEL_2BQZ5GPw/P72Ueob4NzDCv/bMJRyfhj/U0U7s5eJlLdL_2BFDdsI3tf/hKzQjyavf...
834	117.195359	10.5.14.101	34.95.142.247	HTTP	56	POST /9B7mKifdQKW/qmJURXoBUnT5oe/8ij6GtJ1aZtfbCZURJFyZ/LA1Rz1zyEVwIphRb/vwAIX30tvqCtwXT/bfr4N5I68vPbLeMBXp/6y5oop5u/_2Bg_2Fg5C46C_2F0ff...

2021-05-14-Ursnif-infection-traffic.pcap

Packets: 840 · Displayed: 8 (1.0%)

Profile: Default

# Wireshark Analysis of Pcap File



Wireshark · Packet Lengths · 2021-05-14-Ursnif-infection-traffic.pcap

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Packet Lengths	840	961.63	54	1514	0.0071	100%	1.4300	0.506
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	258	54.84	54	78	0.0022	30.71%	0.4200	0.506
80-159	11	98.09	81	122	0.0001	1.31%	0.0200	114.688
160-319	5	269.20	236	314	0.0000	0.60%	0.0100	0.189
320-639	20	505.80	337	631	0.0002	2.38%	0.0200	96.049
640-1279	79	1110.05	677	1202	0.0007	9.40%	0.1400	0.427
1280-2559	467	1484.77	1280	1514	0.0039	55.60%	0.9100	0.506
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Display filter:

# Wireshark Statistics (Filtered)

Wireshark - Capture File Properties - 2021-05-14-Ursnif-infection-traffic.pcap

Details

**File**

Name: C:\Users\maris\Downloads\2021-05-14-Ursnif-traffic-and-malware-and-IOCs\2021-05-14-Ursnif-traffic-and-malware-and-IOCs\2021-05-14-Ursnif-infection-traffic.pcap  
Length: 821 kB  
Hash (SHA256): d8121c60f63cbbab4f04b466395ced4548591fc1b29de74637eeb5dae585fd7e  
Hash (SHA1): 28d316f823cd1247e7e4a68690cfa1b67055183  
Format: Wireshark/tcpdump/... - pcap  
Encapsulation: Ethernet  
Snapshot length: 65535

**Time**

First packet: 2021-05-14 10:56:49  
Last packet: 2021-05-14 10:58:47  
Elapsed: 00:01:58

**Capture**

Hardware: Unknown  
OS: Unknown  
Application: Unknown

**Interfaces**

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

**Statistics**

Measurement	Captured	Displayed	Marked
Packets	840	8 (1.0%)	—
Time span, s	118.317	117.006	—
Average pps	7.1	0.1	—
Average packet size, B	962	436	—
Bytes	807773	3490 (0.4%)	0
Average bytes/s	6827	29	—
Average bits/s	54 k	238	—

Refresh Edit Comments Close Copy To Clipboard Help



# 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](https://github.com/mwchavez/IDS_DF_F2025_Project_MC_MT_DP)

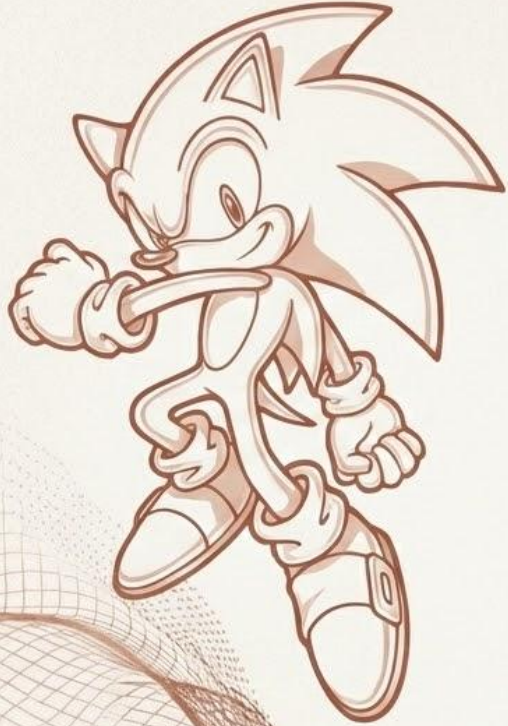
# Future Status of the project

- 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!!

