Assignment 1:
Project analysis of data traffic flows

CYB60004-Networks and Cybersecurity Frameworks

Pulkit Patel
103139787

Contents

Executive summary

This executive summary gives a comprehensive overview of Finmed Financial Fusion's cybersecurity issue investigation. The inquiry was launched following the discovery of a potentially malicious file on the organization's FTP server, which prompted worries about the security of our sensitive data. The primary goal of the contractor heading this investigation was to ascertain the nature of the event, estimate its impact, and offer mitigating actions to enhance our cybersecurity posture.

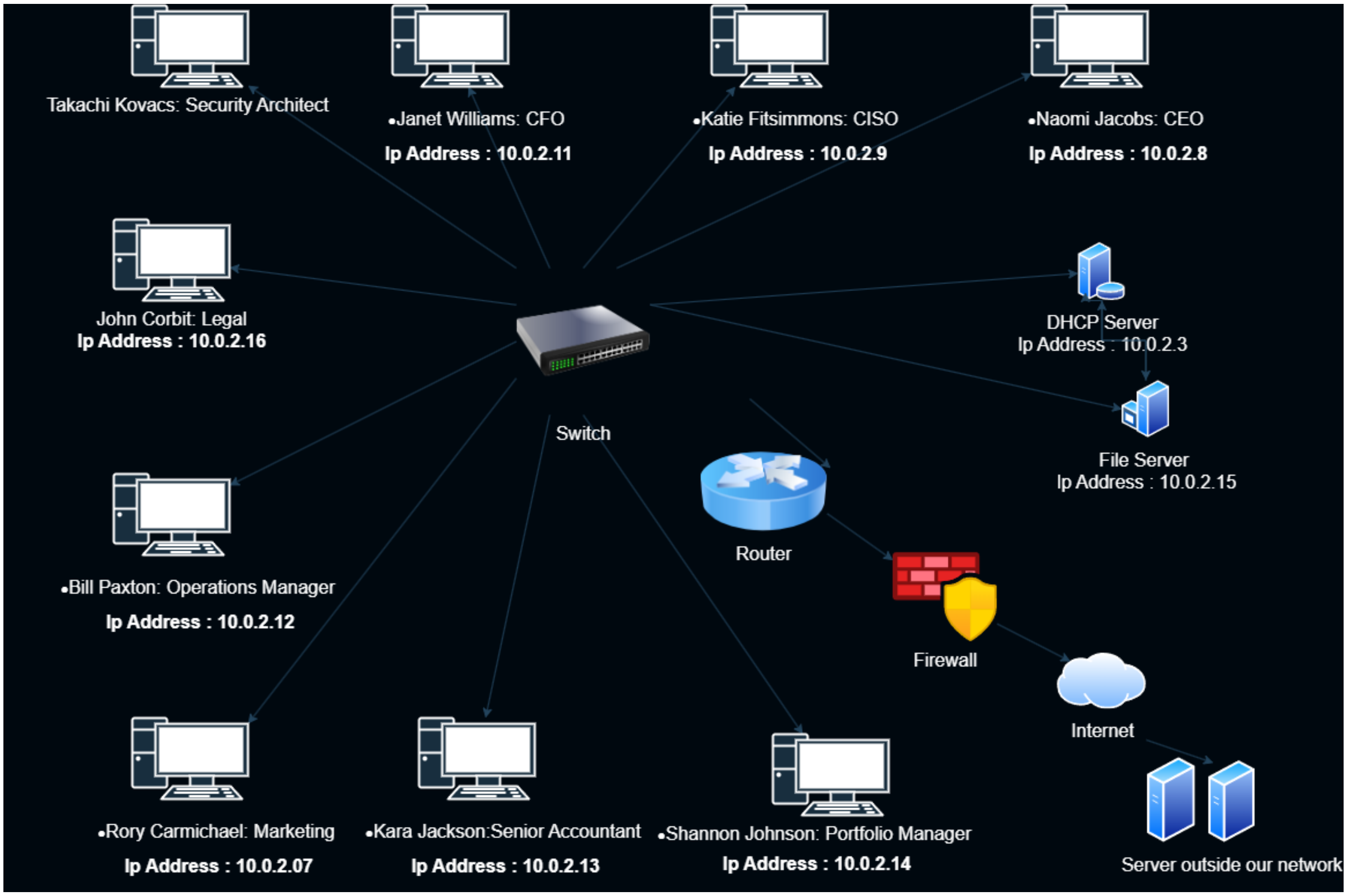
Important Findings:

- On the FTP server, a suspicious malware file was discovered, posing a severe danger to the confidentiality, integrity, and availability of our data.
- Anomalies and possible ports of entry for the virus were identified using network captures.
- A list of employee accounts that needed to be investigated further was developed, raising worries about internal staff disputes.
- The event exposed security flaws and vulnerabilities in our network architecture.

Introduction

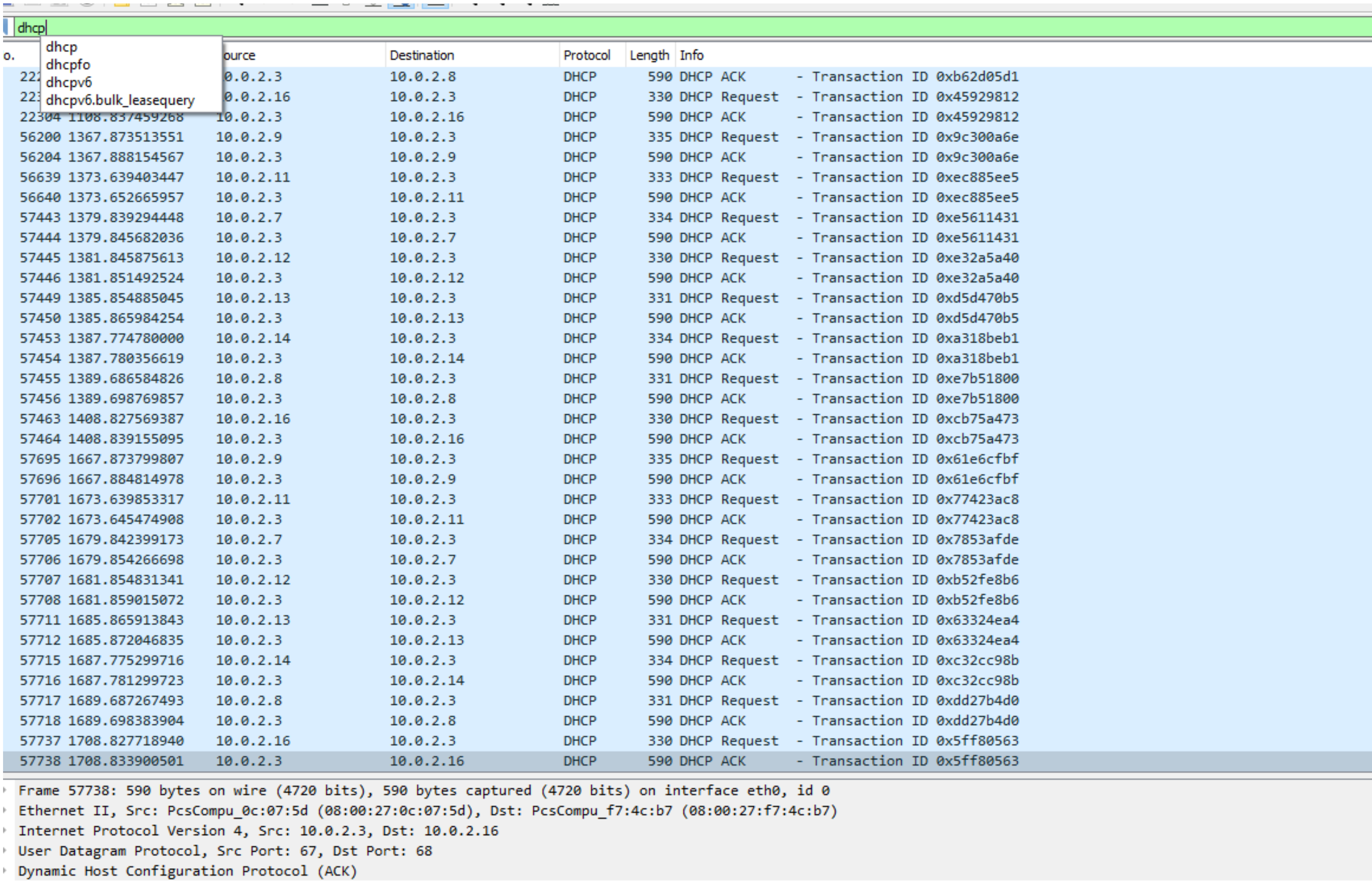
Finmed Financial Fusion is a highly renowned financial organization situated in Melbourne, Australia. To improve brand and service quality as a sponsor of the annual Finmed Cup and under the innovative leadership of our outstanding CEO, Naomi Jacobs. With plans to grow our presence in additional states, it is critical that we retain the highest level of security and client confidence. The enquiry is centered on the discovery of a suspicious malware file on our FTP server. The significance of such an incident cannot be overstated, as it threatens the security, integrity, and availability of our sensitive data. Given this, the Head Office has ordered an internal inquiry, and I have had the honor of being assigned this vital responsibility. During my investigation, I worked closely with the IT team and studied network captures to learn more about the origin and scope of the issue. A list of staff accounts requiring additional investigation was also given, mandating an evaluation of employee participation and access credentials. I also considered recent internal staff disagreements, which might have an impact on our overall cybersecurity posture. Throughout this overview, I will try to describe the investigation's intricacies in simple and straightforward words. My goal is to ensure that all members of this distinguished audience, regardless of technical knowledge, understand the seriousness of the problem and the steps necessary to protect our organization against such dangers in the future. Before I continue, I'd want to thank Immersive Labs for the great cybersecurity training and refresher courses I took, which surely prepared me for this difficult assignment. Without further ado, let us get to the heart of the matter, as I give a comprehensive report on the cybersecurity event and its ramifications for Finmed Financial Fusion.

Network Diagram



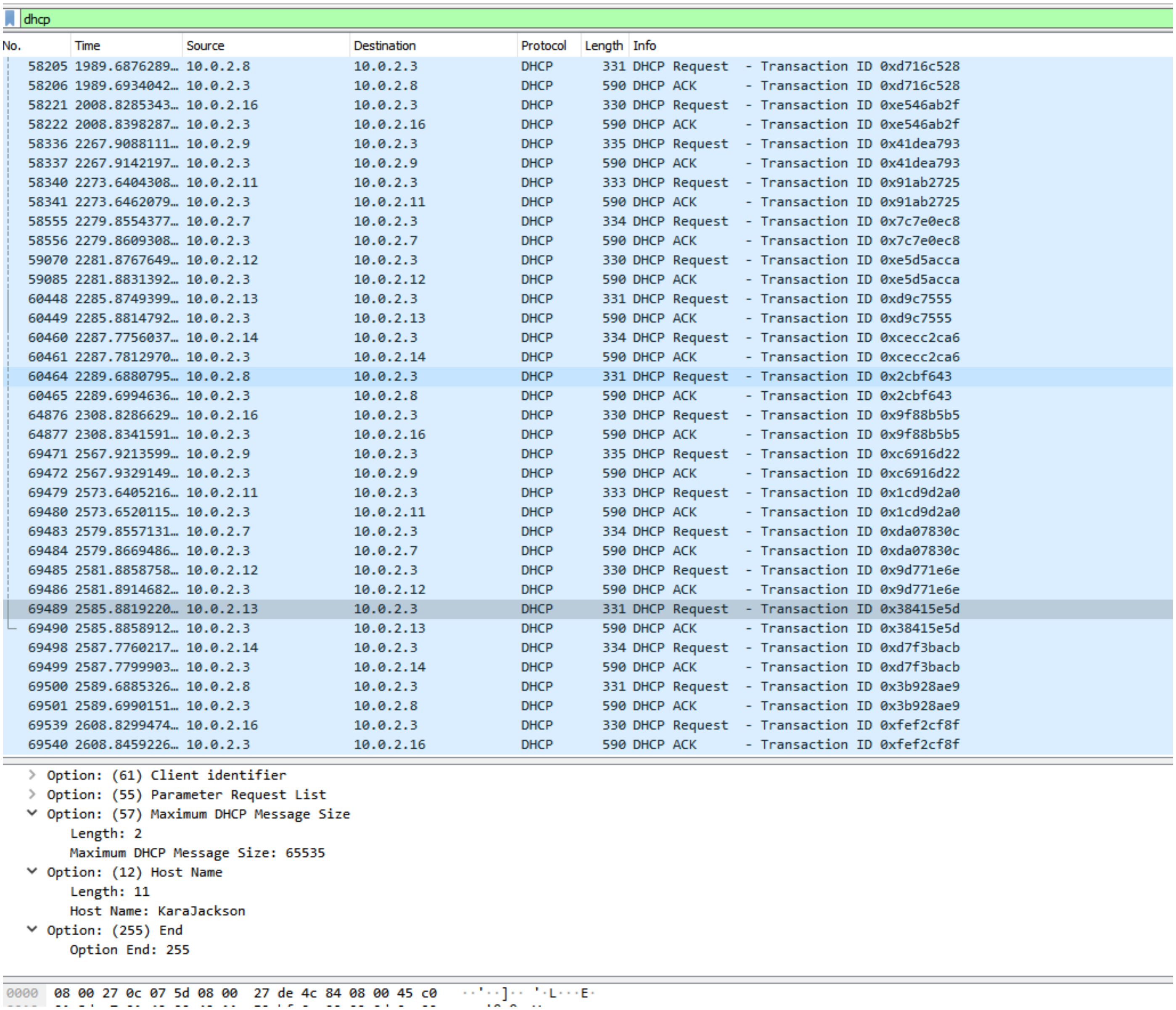
DHCP Evaluation.

- DHCP is used to assign IP addresses to various network devices. It is a client-server protocol that is commonly used in networking to obtain the IP address, default gateway, and subnet mask for machines on the network.
- After filtering the DHCP in Wireshark, the record of all the staff members who are utilizing the company's server and making the request for a New IP address or to renew their IP when the lease duration of IP is over 75% is displayed. Essentially, in the DHCP analysis, I discovered the IP addresses of all staff members in the DHCP request as well as the username by extending option 12.



```
o.                        ource              Destination        Protocol  Length Info
  222                     0.0.2.3            10.0.2.8           DHCP      590 DHCP ACK      - Transaction ID 0xb62d05d1
  223                     0.0.2.16           10.0.2.3           DHCP      330 DHCP Request  - Transaction ID 0x45929812
  22304 1108.837459268    10.0.2.3           10.0.2.16          DHCP      590 DHCP ACK      - Transaction ID 0x45929812
  56200 1367.873513551    10.0.2.9           10.0.2.3           DHCP      335 DHCP Request  - Transaction ID 0x9c300a6e
  56204 1367.888154567    10.0.2.3           10.0.2.9           DHCP      590 DHCP ACK      - Transaction ID 0x9c300a6e
  56639 1373.639403447    10.0.2.11          10.0.2.3           DHCP      333 DHCP Request  - Transaction ID 0xec885ee5
  56640 1373.652665957    10.0.2.3           10.0.2.11          DHCP      590 DHCP ACK      - Transaction ID 0xec885ee5
  57443 1379.839294448    10.0.2.7           10.0.2.3           DHCP      334 DHCP Request  - Transaction ID 0xe5611431
  57444 1379.845682036    10.0.2.3           10.0.2.7           DHCP      590 DHCP ACK      - Transaction ID 0xe5611431
  57445 1381.845875613    10.0.2.12          10.0.2.3           DHCP      330 DHCP Request  - Transaction ID 0xe32a5a40
  57446 1381.851492524    10.0.2.3           10.0.2.12          DHCP      590 DHCP ACK      - Transaction ID 0xe32a5a40
  57449 1385.854885045    10.0.2.13          10.0.2.3           DHCP      331 DHCP Request  - Transaction ID 0xd5d470b5
  57450 1385.865984254    10.0.2.3           10.0.2.13          DHCP      590 DHCP ACK      - Transaction ID 0xd5d470b5
  57453 1387.774780000    10.0.2.14          10.0.2.3           DHCP      334 DHCP Request  - Transaction ID 0xa318beb1
  57454 1387.780356619    10.0.2.3           10.0.2.14          DHCP      590 DHCP ACK      - Transaction ID 0xa318beb1
  57455 1389.686584826    10.0.2.8           10.0.2.3           DHCP      331 DHCP Request  - Transaction ID 0xe7b51800
  57456 1389.698769857    10.0.2.3           10.0.2.8           DHCP      590 DHCP ACK      - Transaction ID 0xe7b51800
  57463 1408.827569387    10.0.2.16          10.0.2.3           DHCP      330 DHCP Request  - Transaction ID 0xcb75a473
  57464 1408.839155095    10.0.2.3           10.0.2.16          DHCP      590 DHCP ACK      - Transaction ID 0xcb75a473
  57695 1667.873799807    10.0.2.9           10.0.2.3           DHCP      335 DHCP Request  - Transaction ID 0x61e6cfbf
  57696 1667.884814978    10.0.2.3           10.0.2.9           DHCP      590 DHCP ACK      - Transaction ID 0x61e6cfbf
  57701 1673.639853317    10.0.2.11          10.0.2.3           DHCP      333 DHCP Request  - Transaction ID 0x77423ac8
  57702 1673.645474908    10.0.2.3           10.0.2.11          DHCP      590 DHCP ACK      - Transaction ID 0x77423ac8
  57705 1679.842399173    10.0.2.7           10.0.2.3           DHCP      334 DHCP Request  - Transaction ID 0x7853afde
  57706 1679.854266698    10.0.2.3           10.0.2.7           DHCP      590 DHCP ACK      - Transaction ID 0x7853afde
  57707 1681.854831341    10.0.2.12          10.0.2.3           DHCP      330 DHCP Request  - Transaction ID 0xb52fe8b6
  57708 1681.859015072    10.0.2.3           10.0.2.12          DHCP      590 DHCP ACK      - Transaction ID 0xb52fe8b6
  57711 1685.865913843    10.0.2.13          10.0.2.3           DHCP      331 DHCP Request  - Transaction ID 0x63324ea4
  57712 1685.872046835    10.0.2.3           10.0.2.13          DHCP      590 DHCP ACK      - Transaction ID 0x63324ea4
  57715 1687.775299716    10.0.2.14          10.0.2.3           DHCP      334 DHCP Request  - Transaction ID 0xc32cc98b
  57716 1687.781299723    10.0.2.3           10.0.2.14          DHCP      590 DHCP ACK      - Transaction ID 0xc32cc98b
  57717 1689.687267493    10.0.2.8           10.0.2.3           DHCP      331 DHCP Request  - Transaction ID 0xdd27b4d0
  57718 1689.698383904    10.0.2.3           10.0.2.8           DHCP      590 DHCP ACK      - Transaction ID 0xdd27b4d0
  57737 1708.827718940    10.0.2.16          10.0.2.3           DHCP      330 DHCP Request  - Transaction ID 0x5ff80563
  57738 1708.833900501    10.0.2.3           10.0.2.16          DHCP      590 DHCP ACK      - Transaction ID 0x5ff80563
```

```
Frame 57738: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0c:07:5d (08:00:27:0c:07:5d), Dst: PcsCompu_f7:4c:b7 (08:00:27:f7:4c:b7)
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.16
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
```



```
dhcp
No.   Time            Source      Destination  Protocol  Length Info
58205 1989.6876289… 10.0.2.8     10.0.2.3     DHCP      331 DHCP Request  - Transaction ID 0xd716c528
58206 1989.6934042… 10.0.2.3     10.0.2.8     DHCP      590 DHCP ACK      - Transaction ID 0xd716c528
58221 2008.8285343… 10.0.2.16    10.0.2.3     DHCP      330 DHCP Request  - Transaction ID 0xe546ab2f
58222 2008.8398287… 10.0.2.3     10.0.2.16    DHCP      590 DHCP ACK      - Transaction ID 0xe546ab2f
58336 2267.9088111… 10.0.2.9     10.0.2.3     DHCP      335 DHCP Request  - Transaction ID 0x41dea793
58337 2267.9142197… 10.0.2.3     10.0.2.9     DHCP      590 DHCP ACK      - Transaction ID 0x41dea793
58340 2273.6404308… 10.0.2.11    10.0.2.3     DHCP      333 DHCP Request  - Transaction ID 0x91ab2725
58341 2273.6462079… 10.0.2.3     10.0.2.11    DHCP      590 DHCP ACK      - Transaction ID 0x91ab2725
58555 2279.8554377… 10.0.2.7     10.0.2.3     DHCP      334 DHCP Request  - Transaction ID 0x7c7e0ec8
58556 2279.8609308… 10.0.2.3     10.0.2.7     DHCP      590 DHCP ACK      - Transaction ID 0x7c7e0ec8
59070 2281.8767649… 10.0.2.12    10.0.2.3     DHCP      330 DHCP Request  - Transaction ID 0xe5d5acca
59085 2281.8831392… 10.0.2.3     10.0.2.12    DHCP      590 DHCP ACK      - Transaction ID 0xe5d5acca
60448 2285.8749399… 10.0.2.13    10.0.2.3     DHCP      331 DHCP Request  - Transaction ID 0xd9c7555
60449 2285.8814792… 10.0.2.3     10.0.2.13    DHCP      590 DHCP ACK      - Transaction ID 0xd9c7555
60460 2287.7756037… 10.0.2.14    10.0.2.3     DHCP      334 DHCP Request  - Transaction ID 0xcecc2ca6
60461 2287.7812970… 10.0.2.3     10.0.2.14    DHCP      590 DHCP ACK      - Transaction ID 0xcecc2ca6
60464 2289.6880795… 10.0.2.8     10.0.2.3     DHCP      331 DHCP Request  - Transaction ID 0x2cbf643
60465 2289.6994636… 10.0.2.3     10.0.2.8     DHCP      590 DHCP ACK      - Transaction ID 0x2cbf643
64876 2308.8286629… 10.0.2.16    10.0.2.3     DHCP      330 DHCP Request  - Transaction ID 0x9f88b5b5
64877 2308.8341591… 10.0.2.3     10.0.2.16    DHCP      590 DHCP ACK      - Transaction ID 0x9f88b5b5
69471 2567.9213599… 10.0.2.9     10.0.2.3     DHCP      335 DHCP Request  - Transaction ID 0xc6916d22
69472 2567.9329149… 10.0.2.3     10.0.2.9     DHCP      590 DHCP ACK      - Transaction ID 0xc6916d22
69479 2573.6405216… 10.0.2.11    10.0.2.3     DHCP      333 DHCP Request  - Transaction ID 0x1cd9d2a0
69480 2573.6520115… 10.0.2.3     10.0.2.11    DHCP      590 DHCP ACK      - Transaction ID 0x1cd9d2a0
69483 2579.8557131… 10.0.2.7     10.0.2.3     DHCP      334 DHCP Request  - Transaction ID 0xda07830c
69484 2579.8669486… 10.0.2.3     10.0.2.7     DHCP      590 DHCP ACK      - Transaction ID 0xda07830c
69485 2581.8858758… 10.0.2.12    10.0.2.3     DHCP      330 DHCP Request  - Transaction ID 0x9d771e6e
69486 2581.8914682… 10.0.2.3     10.0.2.12    DHCP      590 DHCP ACK      - Transaction ID 0x9d771e6e
69489 2585.8819220… 10.0.2.13    10.0.2.3     DHCP      331 DHCP Request  - Transaction ID 0x38415e5d
69490 2585.8858912… 10.0.2.3     10.0.2.13    DHCP      590 DHCP ACK      - Transaction ID 0x38415e5d
69498 2587.7760217… 10.0.2.14    10.0.2.3     DHCP      334 DHCP Request  - Transaction ID 0xd7f3bacb
69499 2587.7799903… 10.0.2.3     10.0.2.14    DHCP      590 DHCP ACK      - Transaction ID 0xd7f3bacb
69500 2589.6885326… 10.0.2.8     10.0.2.3     DHCP      331 DHCP Request  - Transaction ID 0x3b928ae9
69501 2589.6990151… 10.0.2.3     10.0.2.8     DHCP      590 DHCP ACK      - Transaction ID 0x3b928ae9
69539 2608.8299474… 10.0.2.16    10.0.2.3     DHCP      330 DHCP Request  - Transaction ID 0xfef2cf8f
69540 2608.8459226… 10.0.2.3     10.0.2.16    DHCP      590 DHCP ACK      - Transaction ID 0xfef2cf8f

  > Option: (61) Client identifier
  > Option: (55) Parameter Request List
  v Option: (57) Maximum DHCP Message Size
        Length: 2
        Maximum DHCP Message Size: 65535
  v Option: (12) Host Name
        Length: 11
        Host Name: KaraJackson
  v Option: (255) End
        Option End: 255

0000  08 00 27 0c 07 5d 08 00  27 de 4c 84 08 00 45 c0   ··'··]·· '·L···E·
```

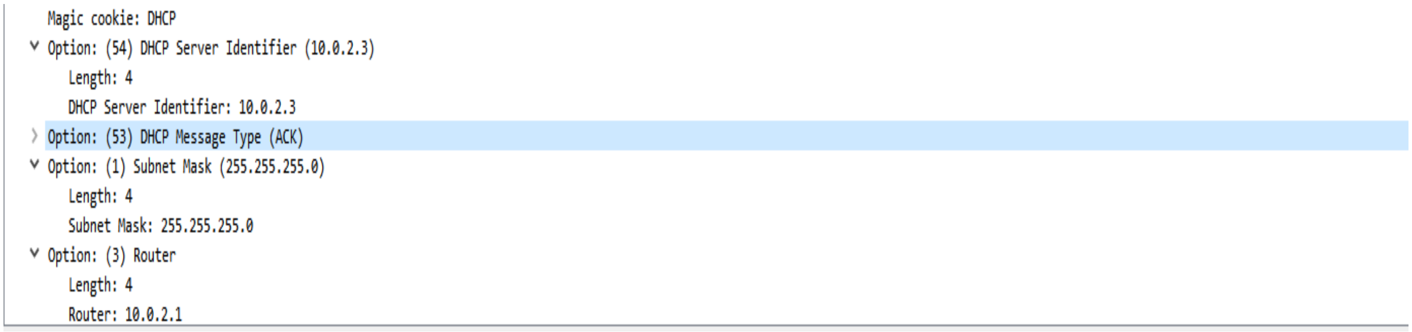
The IP addresses of the staff members discovered through the DHCP analysis are listed below.

- Naomi Jacobs: CEO **10.0.2.8**
- Katie Fitsimmons: CISO **10.0.2.9**
- Janet Williams: CFO **10.0.2.11**
- Takachi Kovacs: Security Architect **Not present in DHCP Analysis**
- John Corbit: Legal **10.0.2.16**
- Bill Paxton: Operations Manager **10.0.2.12**
- Rory Carmichael: Marketing **10.0.2.7**
- Kara Jackson: Senior Accountant **10.0.2.13**
- Shannon Johnson: Portfolio Manager **10.0.2.14**

Takachi Kovacs' IP address may not be discovered in DHCP filtering for the following reasons:

1) He may be using a different computer or network, or he may be absent from the workplace.
2) He might be utilizing the static IP address he assigned himself.

By selecting acknowledge packet in DHCP analysis, you may locate DHCP and the default gateway.

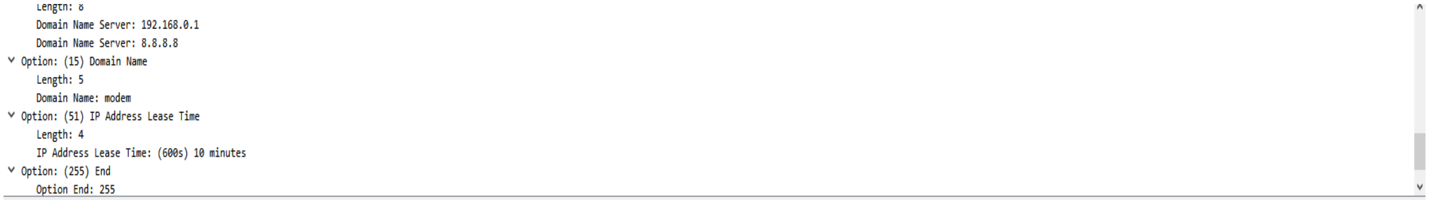


```
   Magic cookie: DHCP
⌄  Option: (54) DHCP Server Identifier (10.0.2.3)
      Length: 4
      DHCP Server Identifier: 10.0.2.3
›  Option: (53) DHCP Message Type (ACK)
⌄  Option: (1) Subnet Mask (255.255.255.0)
      Length: 4
      Subnet Mask: 255.255.255.0
⌄  Option: (3) Router
      Length: 4
      Router: 10.0.2.1
```

The IP address of the DHCP server can be found in option 54, which is 10.0.2.3, and the default gateway can be found in option 3, which is 10.0.2.1.

The DNS IP address and IP leasing time might potentially be obtained in the acknowledgement packet.

The internal network IP address is 192.168.0.1, and Google DNS is 8.8.8.8.

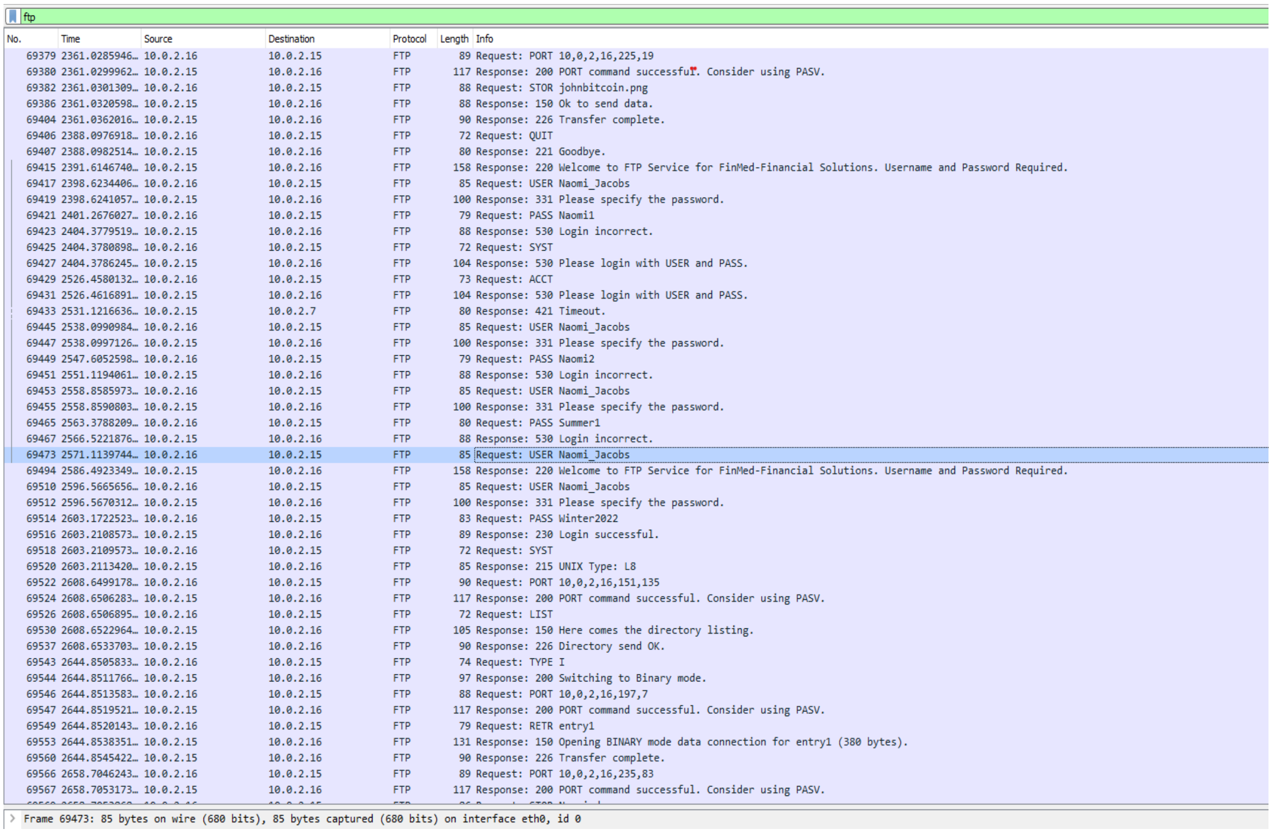


```
      Length: 8
      Domain Name Server: 192.168.0.1
      Domain Name Server: 8.8.8.8
⌄  Option: (15) Domain Name
      Length: 5
      Domain Name: modem
⌄  Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (600s) 10 minutes
⌄  Option: (255) End
      Option End: 255
```

FTP analysis

- FTP, or File Transfer Protocol, is a network protocol used to transfer files from a client to a server across a TCP/IP-based network, such as the internet or a local area network (LAN). When I filter the FTP in wireshark, it displays the network traffic as well as all login actions for all staff users. It also displays the FTP request and response interaction. You may also monitor internet activity by looking at the originating IP address and noting any unusual activity or unwanted network traffic.

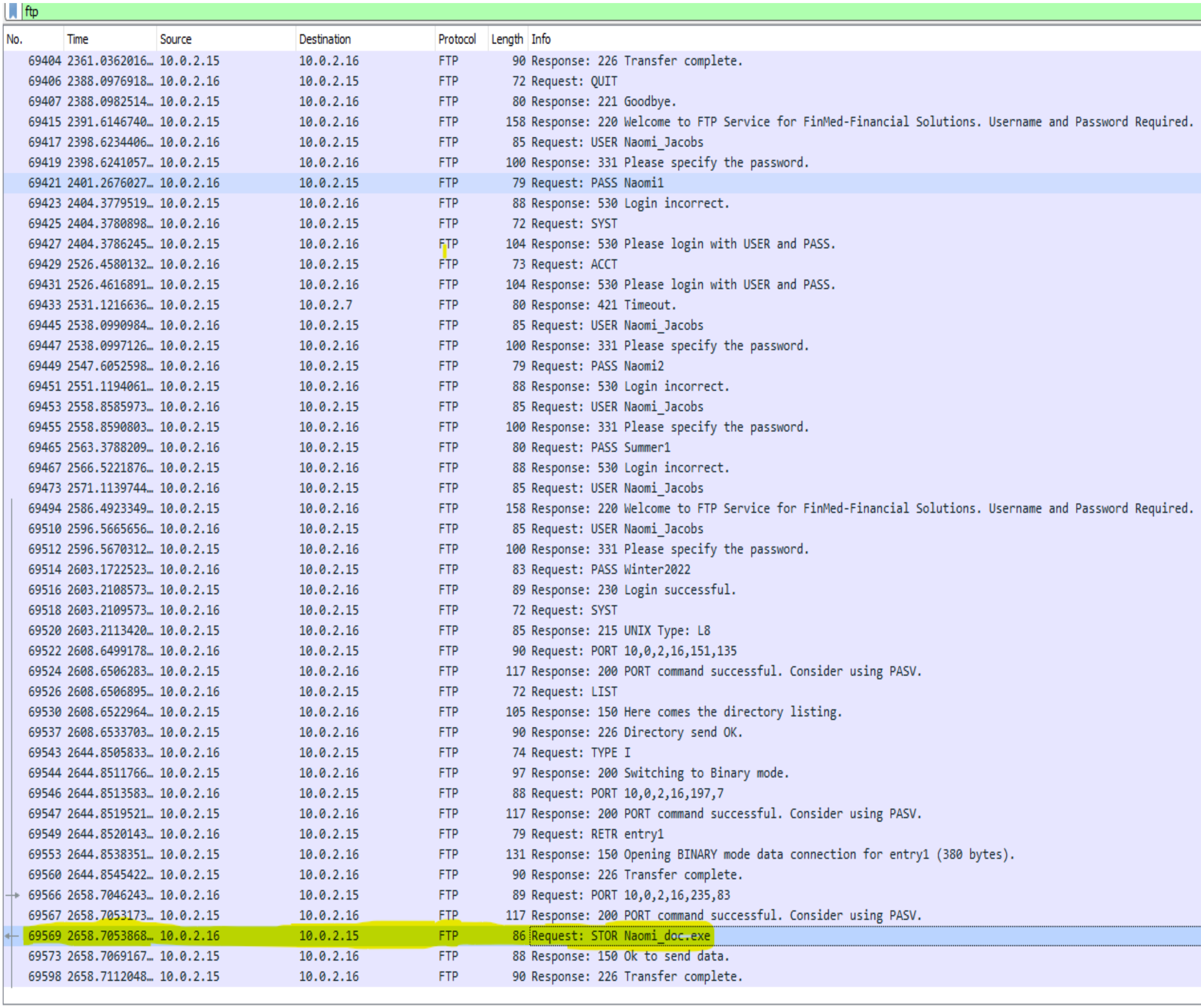
- -FTP analysis in Wireshark is a handy troubleshooting tool that may help you analyze and diagnose problems with FTP connections, authentication difficulties, failed data transfers, and more. It also allows you to ensure that FTP traffic adheres to your company's security rules. You may use Wireshark's filters to focus just on FTP activity within recorded packets. This helps you to concentrate on and isolate FTP-related packets while dealing with large capture files containing many protocols.



```
ftp
No.   Time            Source         Destination    Protocol  Length Info
69379 2361.0285946… 10.0.2.16      10.0.2.15      FTP        89 Request: PORT 10,0,2,16,225,19
69380 2361.0299962… 10.0.2.15      10.0.2.16      FTP       117 Response: 200 PORT command successful. Consider using PASV.
69382 2361.0301309… 10.0.2.16      10.0.2.15      FTP        88 Request: STOR johnbitcoin.png
69386 2361.0320598… 10.0.2.15      10.0.2.16      FTP        88 Response: 150 Ok to send data.
69404 2361.0362016… 10.0.2.15      10.0.2.16      FTP        90 Response: 226 Transfer complete.
69406 2388.0976918… 10.0.2.16      10.0.2.15      FTP        72 Request: QUIT
69407 2388.0982514… 10.0.2.15      10.0.2.16      FTP        80 Response: 221 Goodbye.
69415 2391.6146740… 10.0.2.15      10.0.2.16      FTP       158 Response: 220 Welcome to FTP Service for FinMed-Financial Solutions. Username and Password Required.
69417 2398.6234406… 10.0.2.16      10.0.2.15      FTP        85 Request: USER Naomi_Jacobs
69419 2398.6241057… 10.0.2.15      10.0.2.16      FTP       100 Response: 331 Please specify the password.
69421 2401.2676027… 10.0.2.16      10.0.2.15      FTP        79 Request: PASS Naomi1
69423 2404.3779519… 10.0.2.15      10.0.2.16      FTP        88 Response: 530 Login incorrect.
69425 2404.3780898… 10.0.2.16      10.0.2.15      FTP        72 Request: SYST
69427 2404.3786245… 10.0.2.15      10.0.2.16      FTP       104 Response: 530 Please login with USER and PASS.
69429 2526.4580132… 10.0.2.16      10.0.2.15      FTP        73 Request: ACCT
69431 2526.4616891… 10.0.2.15      10.0.2.16      FTP       104 Response: 530 Please login with USER and PASS.
69433 2531.1216636… 10.0.2.15      10.0.2.7       FTP        80 Response: 421 Timeout.
69445 2538.0990984… 10.0.2.16      10.0.2.15      FTP        85 Request: USER Naomi_Jacobs
69447 2538.0997126… 10.0.2.15      10.0.2.16      FTP       100 Response: 331 Please specify the password.
69449 2547.6052598… 10.0.2.16      10.0.2.15      FTP        79 Request: PASS Naomi2
69451 2551.1194061… 10.0.2.15      10.0.2.16      FTP        88 Response: 530 Login incorrect.
69453 2558.8585973… 10.0.2.16      10.0.2.15      FTP        85 Request: USER Naomi_Jacobs
69455 2558.8590803… 10.0.2.15      10.0.2.16      FTP       100 Response: 331 Please specify the password.
69465 2563.3788209… 10.0.2.16      10.0.2.15      FTP        80 Request: PASS Summer1
69467 2566.5221876… 10.0.2.15      10.0.2.16      FTP        88 Response: 530 Login incorrect.
69473 2571.1139744… 10.0.2.16      10.0.2.15      FTP        85 Request: USER Naomi_Jacobs
69494 2586.4923349… 10.0.2.15      10.0.2.16      FTP       158 Response: 220 Welcome to FTP Service for FinMed-Financial Solutions. Username and Password Required.
69510 2596.5665656… 10.0.2.16      10.0.2.15      FTP        85 Request: USER Naomi_Jacobs
69512 2596.5670312… 10.0.2.15      10.0.2.16      FTP       100 Response: 331 Please specify the password.
69514 2603.1722523… 10.0.2.16      10.0.2.15      FTP        83 Request: PASS Winter2022
69516 2603.2108573… 10.0.2.15      10.0.2.16      FTP        89 Response: 230 Login successful.
69518 2603.2109573… 10.0.2.16      10.0.2.15      FTP        72 Request: SYST
69520 2603.2113420… 10.0.2.15      10.0.2.16      FTP        85 Response: 215 UNIX Type: L8
69522 2608.6499178… 10.0.2.16      10.0.2.15      FTP        90 Request: PORT 10,0,2,16,151,135
69524 2608.6506283… 10.0.2.15      10.0.2.16      FTP       117 Response: 200 PORT command successful. Consider using PASV.
69526 2608.6506895… 10.0.2.16      10.0.2.15      FTP        72 Request: LIST
69530 2608.6522964… 10.0.2.15      10.0.2.16      FTP       105 Response: 150 Here comes the directory listing.
69537 2608.6533703… 10.0.2.15      10.0.2.16      FTP        90 Response: 226 Directory send OK.
69543 2644.8505833… 10.0.2.16      10.0.2.15      FTP        74 Request: TYPE I
69544 2644.8511766… 10.0.2.15      10.0.2.16      FTP        97 Response: 200 Switching to Binary mode.
69546 2644.8513583… 10.0.2.16      10.0.2.15      FTP        88 Request: PORT 10,0,2,16,197,7
69547 2644.8519521… 10.0.2.15      10.0.2.16      FTP       117 Response: 200 PORT command successful. Consider using PASV.
69549 2644.8520143… 10.0.2.16      10.0.2.15      FTP        79 Request: RETR entry1
69553 2644.8538351… 10.0.2.15      10.0.2.16      FTP       131 Response: 150 Opening BINARY mode data connection for entry1 (380 bytes).
69560 2644.8545422… 10.0.2.15      10.0.2.16      FTP        90 Response: 226 Transfer complete.
69566 2658.7046243… 10.0.2.16      10.0.2.15      FTP        89 Request: PORT 10,0,2,16,235,83
69567 2658.7053173… 10.0.2.15      10.0.2.16      FTP       117 Response: 200 PORT command successful. Consider using PASV.

> Frame 69473: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface eth0, id 0
```

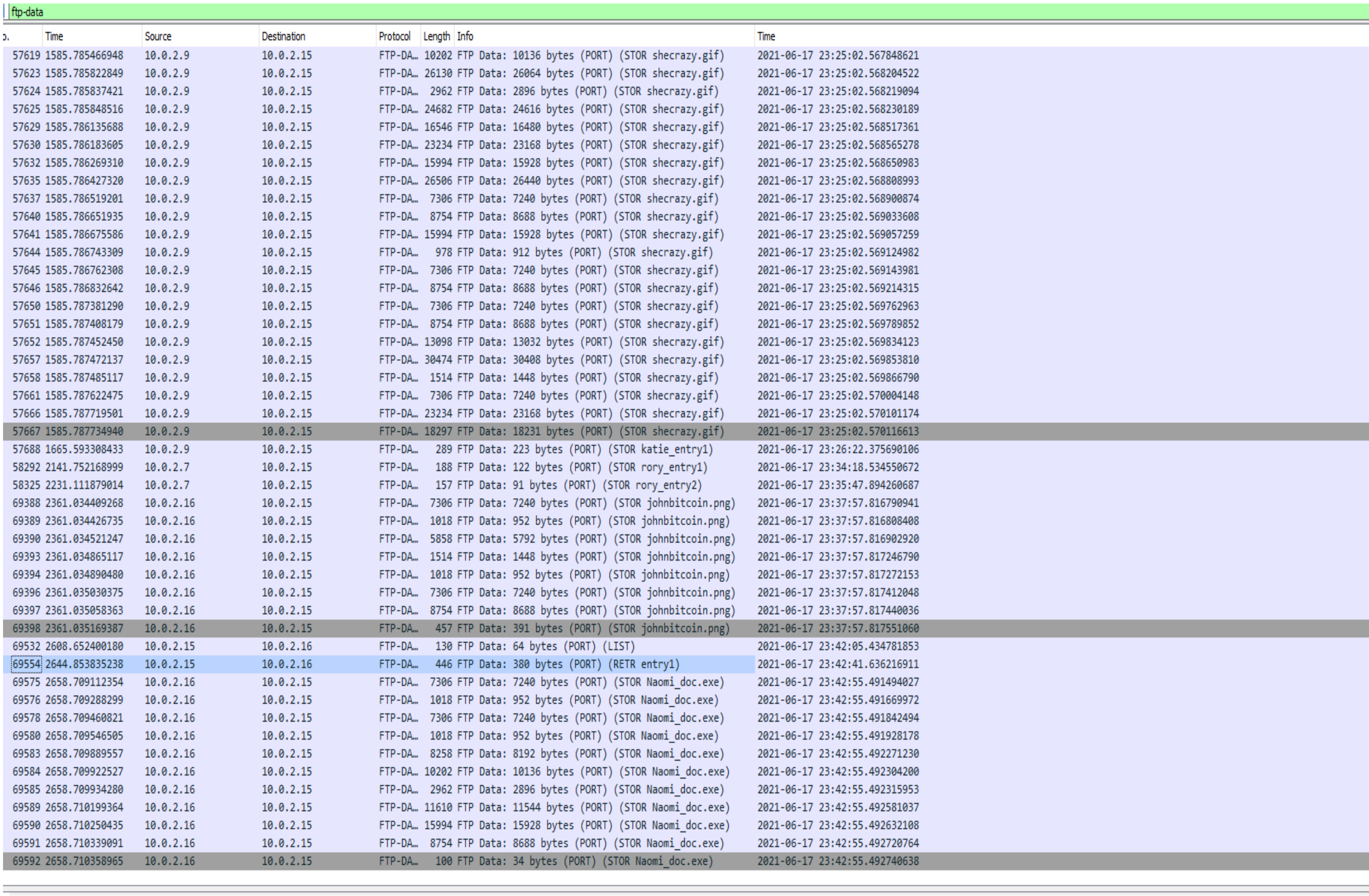
There was suspicious behavior in the FTP analysis when Naomi Jacobs checked in numerous times with a different source IP that belonged to John Corbit (10.0.2.16). There might be various explanations for this, including Naomi Jacobs' malfunctioning gadget and her use of John Corbit's computer, or John Corbit utilizing Naomi's account for unlawful or unpleasant activity. However, the cyber security analyst should take notice of this and investigate further.



```
ftp
No.    Time           Source     Destination  Protocol  Length  Info
 69404 2361.0362016…  10.0.2.15  10.0.2.16    FTP          90 Response: 226 Transfer complete.
 69406 2388.0976918…  10.0.2.16  10.0.2.15    FTP          72 Request: QUIT
 69407 2388.0982514…  10.0.2.15  10.0.2.16    FTP          80 Response: 221 Goodbye.
 69415 2391.6146740…  10.0.2.15  10.0.2.16    FTP         158 Response: 220 Welcome to FTP Service for FinMed-Financial Solutions. Username and Password Required.
 69417 2398.6234406…  10.0.2.16  10.0.2.15    FTP          85 Request: USER Naomi_Jacobs
 69419 2398.6241057…  10.0.2.15  10.0.2.16    FTP         100 Response: 331 Please specify the password.
 69421 2401.2676027…  10.0.2.16  10.0.2.15    FTP          79 Request: PASS Naomi1
 69423 2404.3779519…  10.0.2.15  10.0.2.16    FTP          88 Response: 530 Login incorrect.
 69425 2404.3780898…  10.0.2.16  10.0.2.15    FTP          72 Request: SYST
 69427 2404.3786245…  10.0.2.15  10.0.2.16    FTP         104 Response: 530 Please login with USER and PASS.
 69429 2526.4580132…  10.0.2.16  10.0.2.15    FTP          73 Request: ACCT
 69431 2526.4616891…  10.0.2.15  10.0.2.16    FTP         104 Response: 530 Please login with USER and PASS.
 69433 2531.1216636…  10.0.2.15  10.0.2.7     FTP          80 Response: 421 Timeout.
 69445 2538.0990984…  10.0.2.16  10.0.2.15    FTP          85 Request: USER Naomi_Jacobs
 69447 2538.0997126…  10.0.2.15  10.0.2.16    FTP         100 Response: 331 Please specify the password.
 69449 2547.6052598…  10.0.2.16  10.0.2.15    FTP          79 Request: PASS Naomi2
 69451 2551.1194061…  10.0.2.15  10.0.2.16    FTP          88 Response: 530 Login incorrect.
 69453 2558.8585973…  10.0.2.16  10.0.2.15    FTP          85 Request: USER Naomi_Jacobs
 69455 2558.8590803…  10.0.2.15  10.0.2.16    FTP         100 Response: 331 Please specify the password.
 69465 2563.3788209…  10.0.2.16  10.0.2.15    FTP          80 Request: PASS Summer1
 69467 2566.5221876…  10.0.2.15  10.0.2.16    FTP          88 Response: 530 Login incorrect.
 69473 2571.1139744…  10.0.2.16  10.0.2.15    FTP          85 Request: USER Naomi_Jacobs
 69494 2586.4923349…  10.0.2.15  10.0.2.16    FTP         158 Response: 220 Welcome to FTP Service for FinMed-Financial Solutions. Username and Password Required.
 69510 2596.5665656…  10.0.2.16  10.0.2.15    FTP          85 Request: USER Naomi_Jacobs
 69512 2596.5670312…  10.0.2.15  10.0.2.16    FTP         100 Response: 331 Please specify the password.
 69514 2603.1722523…  10.0.2.16  10.0.2.15    FTP          83 Request: PASS Winter2022
 69516 2603.2108573…  10.0.2.15  10.0.2.16    FTP          89 Response: 230 Login successful.
 69518 2603.2109573…  10.0.2.16  10.0.2.15    FTP          72 Request: SYST
 69520 2603.2113420…  10.0.2.15  10.0.2.16    FTP          85 Response: 215 UNIX Type: L8
 69522 2608.6499178…  10.0.2.16  10.0.2.15    FTP          90 Request: PORT 10,0,2,16,151,135
 69524 2608.6506283…  10.0.2.15  10.0.2.16    FTP         117 Response: 200 PORT command successful. Consider using PASV.
 69526 2608.6506895…  10.0.2.16  10.0.2.15    FTP          72 Request: LIST
 69530 2608.6522964…  10.0.2.15  10.0.2.16    FTP         105 Response: 150 Here comes the directory listing.
 69537 2608.6533703…  10.0.2.15  10.0.2.16    FTP          90 Response: 226 Directory send OK.
 69543 2644.8505833…  10.0.2.16  10.0.2.15    FTP          74 Request: TYPE I
 69544 2644.8511766…  10.0.2.15  10.0.2.16    FTP          97 Response: 200 Switching to Binary mode.
 69546 2644.8513583…  10.0.2.16  10.0.2.15    FTP          88 Request: PORT 10,0,2,16,197,7
 69547 2644.8519521…  10.0.2.15  10.0.2.16    FTP         117 Response: 200 PORT command successful. Consider using PASV.
 69549 2644.8520143…  10.0.2.16  10.0.2.15    FTP          79 Request: RETR entry1
 69553 2644.8538351…  10.0.2.15  10.0.2.16    FTP         131 Response: 150 Opening BINARY mode data connection for entry1 (380 bytes).
 69560 2644.8545422…  10.0.2.15  10.0.2.16    FTP          90 Response: 226 Transfer complete.
 69566 2658.7046243…  10.0.2.16  10.0.2.15    FTP          89 Request: PORT 10,0,2,16,235,83
 69567 2658.7053173…  10.0.2.15  10.0.2.16    FTP         117 Response: 200 PORT command successful. Consider using PASV.
 69569 2658.7053868…  10.0.2.16  10.0.2.15    FTP          86 Request: STOR Naomi_doc.exe
 69573 2658.7069167…  10.0.2.15  10.0.2.16    FTP          88 Response: 150 Ok to send data.
 69598 2658.7112048…  10.0.2.15  10.0.2.16    FTP          90 Response: 226 Transfer complete.
```

John Corbit has tried multiple passwords to access Naomi's account. After a successful login, he saved the naomi_doc.exe file, raising the specter of infection.

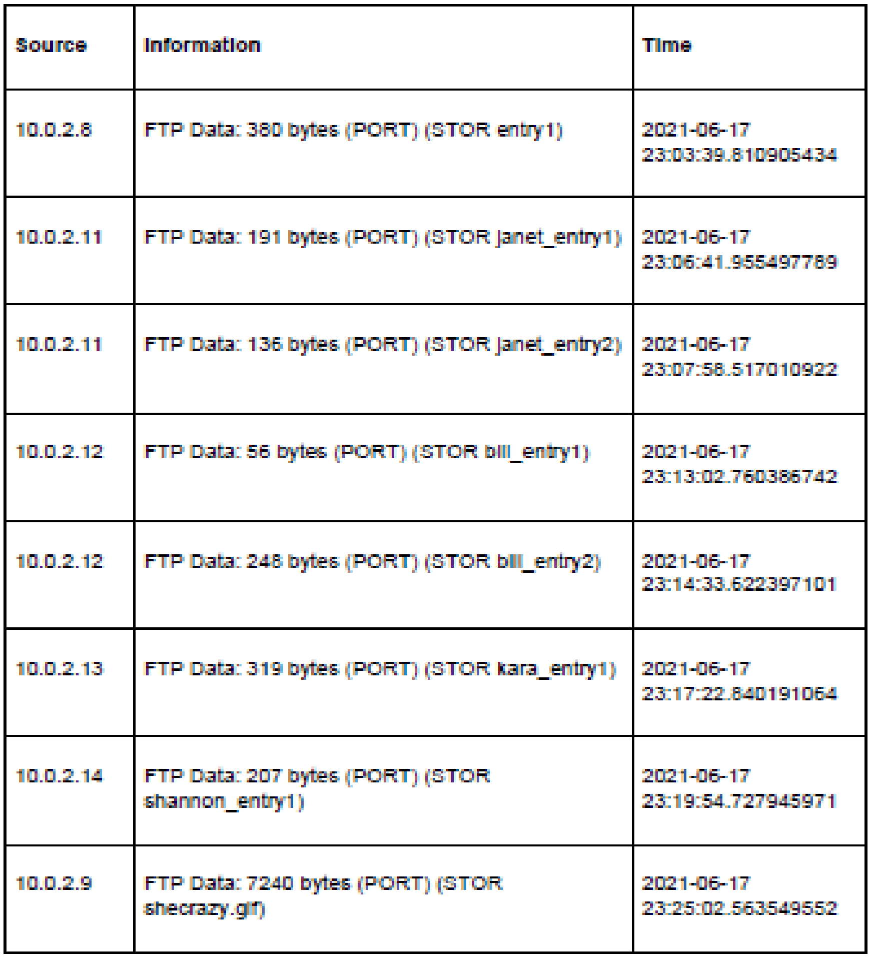
FTP file transfers



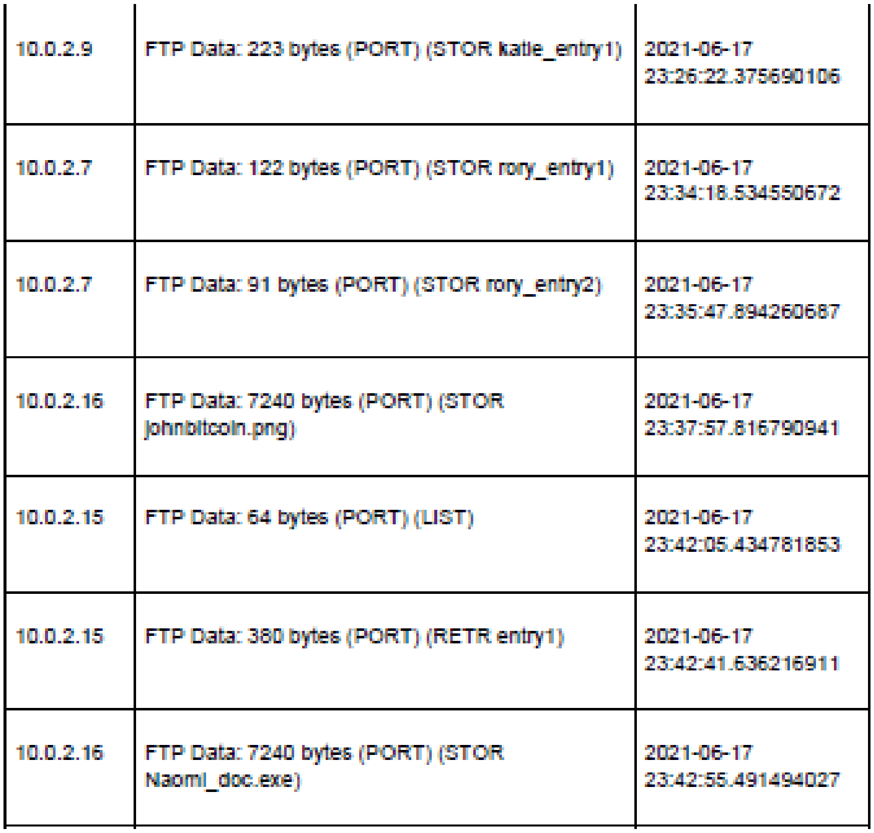
ftp-data

o.	Time	Source	Destination	Protocol	Length	Info	Time
57619	1585.785466948	10.0.2.9	10.0.2.15	FTP-DA…	10202	FTP Data: 10136 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.567848621
57623	1585.785822849	10.0.2.9	10.0.2.15	FTP-DA…	26130	FTP Data: 26064 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568204522
57624	1585.785837421	10.0.2.9	10.0.2.15	FTP-DA…	2962	FTP Data: 2896 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568219094
57625	1585.785848516	10.0.2.9	10.0.2.15	FTP-DA…	24682	FTP Data: 24616 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568230189
57629	1585.786135688	10.0.2.9	10.0.2.15	FTP-DA…	16546	FTP Data: 16480 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568517361
57630	1585.786183605	10.0.2.9	10.0.2.15	FTP-DA…	23234	FTP Data: 23168 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568565278
57632	1585.786269310	10.0.2.9	10.0.2.15	FTP-DA…	15994	FTP Data: 15928 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568650983
57635	1585.786427320	10.0.2.9	10.0.2.15	FTP-DA…	26506	FTP Data: 26440 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568808993
57637	1585.786519201	10.0.2.9	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.568900874
57640	1585.786651935	10.0.2.9	10.0.2.15	FTP-DA…	8754	FTP Data: 8688 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569033608
57641	1585.786675586	10.0.2.9	10.0.2.15	FTP-DA…	15994	FTP Data: 15928 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569057259
57644	1585.786743309	10.0.2.9	10.0.2.15	FTP-DA…	978	FTP Data: 912 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569124982
57645	1585.786762308	10.0.2.9	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569143981
57646	1585.786832642	10.0.2.9	10.0.2.15	FTP-DA…	8754	FTP Data: 8688 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569214315
57650	1585.787381290	10.0.2.9	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569762963
57651	1585.787408179	10.0.2.9	10.0.2.15	FTP-DA…	8754	FTP Data: 8688 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569789852
57652	1585.787452450	10.0.2.9	10.0.2.15	FTP-DA…	13098	FTP Data: 13032 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569834123
57657	1585.787472137	10.0.2.9	10.0.2.15	FTP-DA…	30474	FTP Data: 30408 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569853810
57658	1585.787485117	10.0.2.9	10.0.2.15	FTP-DA…	1514	FTP Data: 1448 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.569866790
57661	1585.787622475	10.0.2.9	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.570004148
57666	1585.787719501	10.0.2.9	10.0.2.15	FTP-DA…	23234	FTP Data: 23168 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.570101174
57667	1585.787734940	10.0.2.9	10.0.2.15	FTP-DA…	18297	FTP Data: 18231 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.570116613
57688	1665.593308433	10.0.2.9	10.0.2.15	FTP-DA…	289	FTP Data: 223 bytes (PORT) (STOR katie_entry1)	2021-06-17 23:26:22.375690106
58292	2141.752168999	10.0.2.7	10.0.2.15	FTP-DA…	188	FTP Data: 122 bytes (PORT) (STOR rory_entry1)	2021-06-17 23:34:18.534550672
58325	2231.111879014	10.0.2.7	10.0.2.15	FTP-DA…	157	FTP Data: 91 bytes (PORT) (STOR rory_entry2)	2021-06-17 23:35:47.894260687
69388	2361.034409268	10.0.2.16	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.816790941
69389	2361.034426735	10.0.2.16	10.0.2.15	FTP-DA…	1018	FTP Data: 952 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.816808408
69390	2361.034521247	10.0.2.16	10.0.2.15	FTP-DA…	5858	FTP Data: 5792 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.816902920
69393	2361.034865117	10.0.2.16	10.0.2.15	FTP-DA…	1514	FTP Data: 1448 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.817246790
69394	2361.034890480	10.0.2.16	10.0.2.15	FTP-DA…	1018	FTP Data: 952 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.817272153
69396	2361.035030375	10.0.2.16	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.817412048
69397	2361.035058363	10.0.2.16	10.0.2.15	FTP-DA…	8754	FTP Data: 8688 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.817440036
69398	2361.035169387	10.0.2.16	10.0.2.15	FTP-DA…	457	FTP Data: 391 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.817551060
69532	2608.652400180	10.0.2.15	10.0.2.16	FTP-DA…	130	FTP Data: 64 bytes (PORT) (LIST)	2021-06-17 23:42:05.434781853
69554	2644.853835238	10.0.2.15	10.0.2.16	FTP-DA…	446	FTP Data: 380 bytes (PORT) (RETR entry1)	2021-06-17 23:42:41.636216911
69575	2658.709112354	10.0.2.16	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.491494027
69576	2658.709288299	10.0.2.16	10.0.2.15	FTP-DA…	1018	FTP Data: 952 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.491669972
69578	2658.709460821	10.0.2.16	10.0.2.15	FTP-DA…	7306	FTP Data: 7240 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.491842494
69580	2658.709546505	10.0.2.16	10.0.2.15	FTP-DA…	1018	FTP Data: 952 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.491928178
69583	2658.709889557	10.0.2.16	10.0.2.15	FTP-DA…	8258	FTP Data: 8192 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492271230
69584	2658.709922527	10.0.2.16	10.0.2.15	FTP-DA…	10202	FTP Data: 10136 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492304200
69585	2658.709934280	10.0.2.16	10.0.2.15	FTP-DA…	2962	FTP Data: 2896 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492315953
69589	2658.710199364	10.0.2.16	10.0.2.15	FTP-DA…	11610	FTP Data: 11544 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492581037
69590	2658.710250435	10.0.2.16	10.0.2.15	FTP-DA…	15994	FTP Data: 15928 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492632108
69591	2658.710339091	10.0.2.16	10.0.2.15	FTP-DA…	8754	FTP Data: 8688 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492720764
69592	2658.710358965	10.0.2.16	10.0.2.15	FTP-DA…	100	FTP Data: 34 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.492740638

The data obtained during the FTP -data analysis displays information about the data transfer or data that has been uploaded, including the amount of the data, the source IP address, and the time.



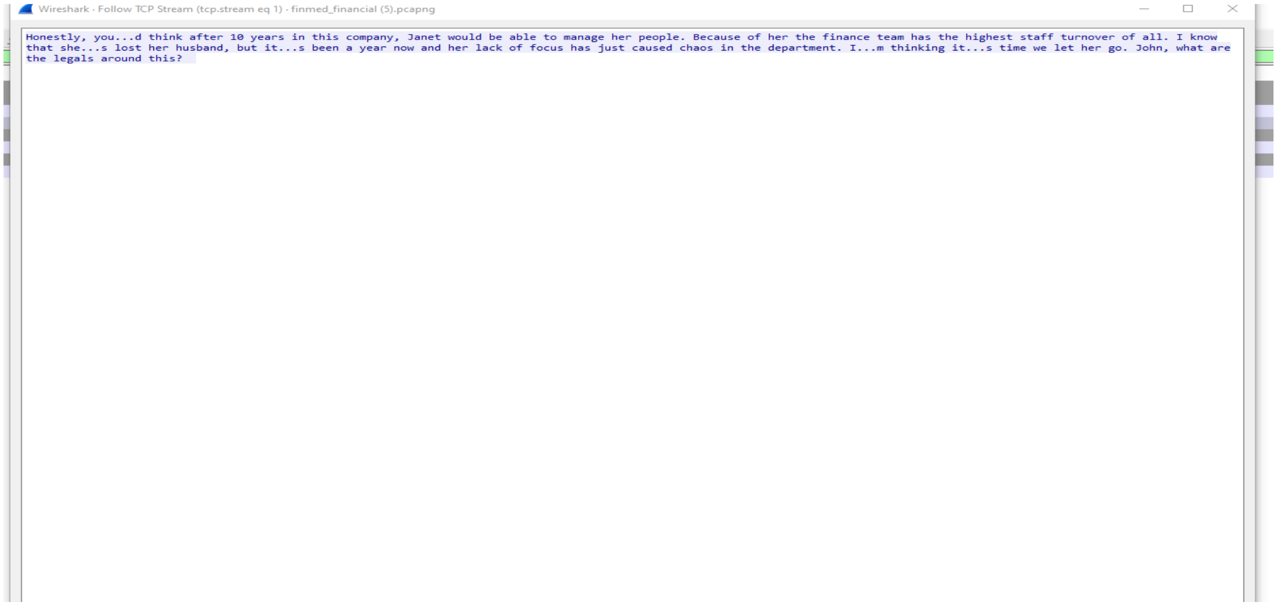
Source	Information	Time
10.0.2.8	FTP Data: 380 bytes (PORT) (STOR entry1)	2021-06-17 23:03:39.810905434
10.0.2.11	FTP Data: 191 bytes (PORT) (STOR janet_entry1)	2021-06-17 23:06:41.955497789
10.0.2.11	FTP Data: 136 bytes (PORT) (STOR janet_entry2)	2021-06-17 23:07:58.517010922
10.0.2.12	FTP Data: 56 bytes (PORT) (STOR bill_entry1)	2021-06-17 23:13:02.760386742
10.0.2.12	FTP Data: 248 bytes (PORT) (STOR bill_entry2)	2021-06-17 23:14:33.622397101
10.0.2.13	FTP Data: 319 bytes (PORT) (STOR kara_entry1)	2021-06-17 23:17:22.840191064
10.0.2.14	FTP Data: 207 bytes (PORT) (STOR shannon_entry1)	2021-06-17 23:19:54.727945971
10.0.2.9	FTP Data: 7240 bytes (PORT) (STOR shecrazy.gif)	2021-06-17 23:25:02.563549552



10.0.2.9	FTP Data: 223 bytes (PORT) (STOR katie_entry1)	2021-06-17 23:26:22.375690106
10.0.2.7	FTP Data: 122 bytes (PORT) (STOR rory_entry1)	2021-06-17 23:34:18.534550672
10.0.2.7	FTP Data: 91 bytes (PORT) (STOR rory_entry2)	2021-06-17 23:35:47.894260687
10.0.2.16	FTP Data: 7240 bytes (PORT) (STOR johnbitcoin.png)	2021-06-17 23:37:57.816790941
10.0.2.15	FTP Data: 64 bytes (PORT) (LIST)	2021-06-17 23:42:05.434781853
10.0.2.15	FTP Data: 380 bytes (PORT) (RETR entry1)	2021-06-17 23:42:41.636216911
10.0.2.16	FTP Data: 7240 bytes (PORT) (STOR Naomi_doc.exe)	2021-06-17 23:42:55.491494027

- - The most crucial finding in FTP-data analysis was that the Naomi_Doc.exe file from source 10.0.2.16 was uploaded 11 times to the FTP server.
- - On the other hand, the information available during the FTP data analysis is extremely private and readily accessible to anybody, which is not a desirable characteristic when considering the security and privacy of all staff members. This information might be misused by anyone, and it could lead to other undesirable behaviors within the firm.

The next snapshot depicts a conversation between staff personnel who are either severely upset with Janet or dislike her for personal or professional reasons. The evidence revealed here is useful and can aid in resolving the ongoing conflicts between staff members.

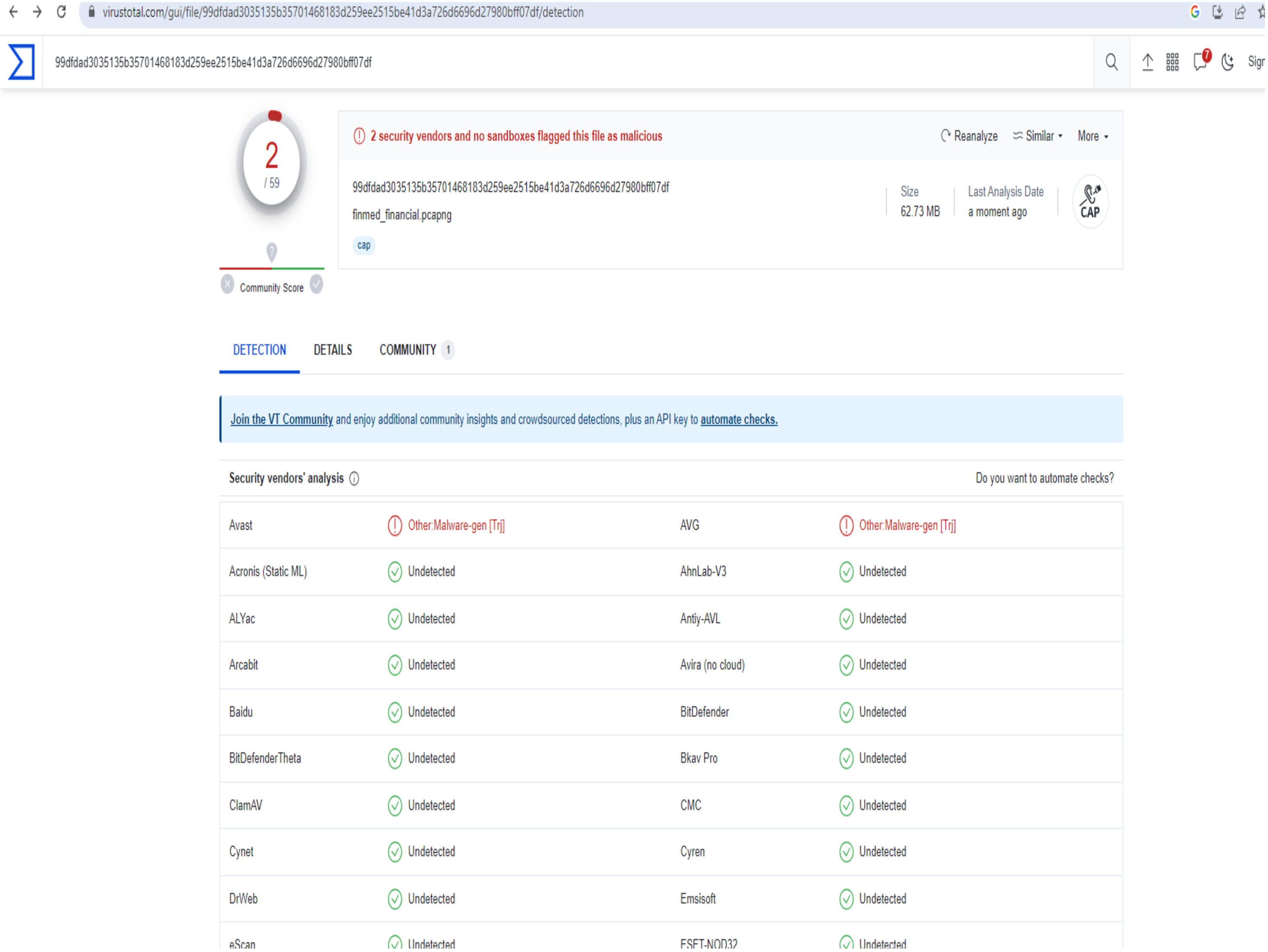


Wireshark · Follow TCP Stream (tcp.stream eq 1) · finmed_financial (5).pcapng

```
Honestly, you...d think after 10 years in this company, Janet would be able to manage her people. Because of her the finance team has the highest staff turnover of all. I know
that she...s lost her husband, but it...s been a year now and her lack of focus has just caused chaos in the department. I...m thinking it...s time we let her go. John, what are
the legals around this?
```

- - The preceding GIF was also discovered in ftp-data analysis, indicating that there is a lot going on between the personnel around Janet. This should surely prompt an enquiry to determine what is going on among all of the workers.
- - On the other hand, the data contained in ftp-data are extremely private and violate a company's privacy policy, as well as calling into question the security element.
-

Malware Check



virustotal.com/gui/file/99dfdad3035135b35701468183d259ee2515be41d3a726d6696d27980bff07df/detection

99dfdad3035135b35701468183d259ee2515be41d3a726d6696d27980bff07df

2
/ 59

2 security vendors and no sandboxes flagged this file as malicious

99dfdad3035135b35701468183d259ee2515be41d3a726d6696d27980bff07df

finmed_financial.pcapng

cap

Size
62.73 MB

Last Analysis Date
a moment ago

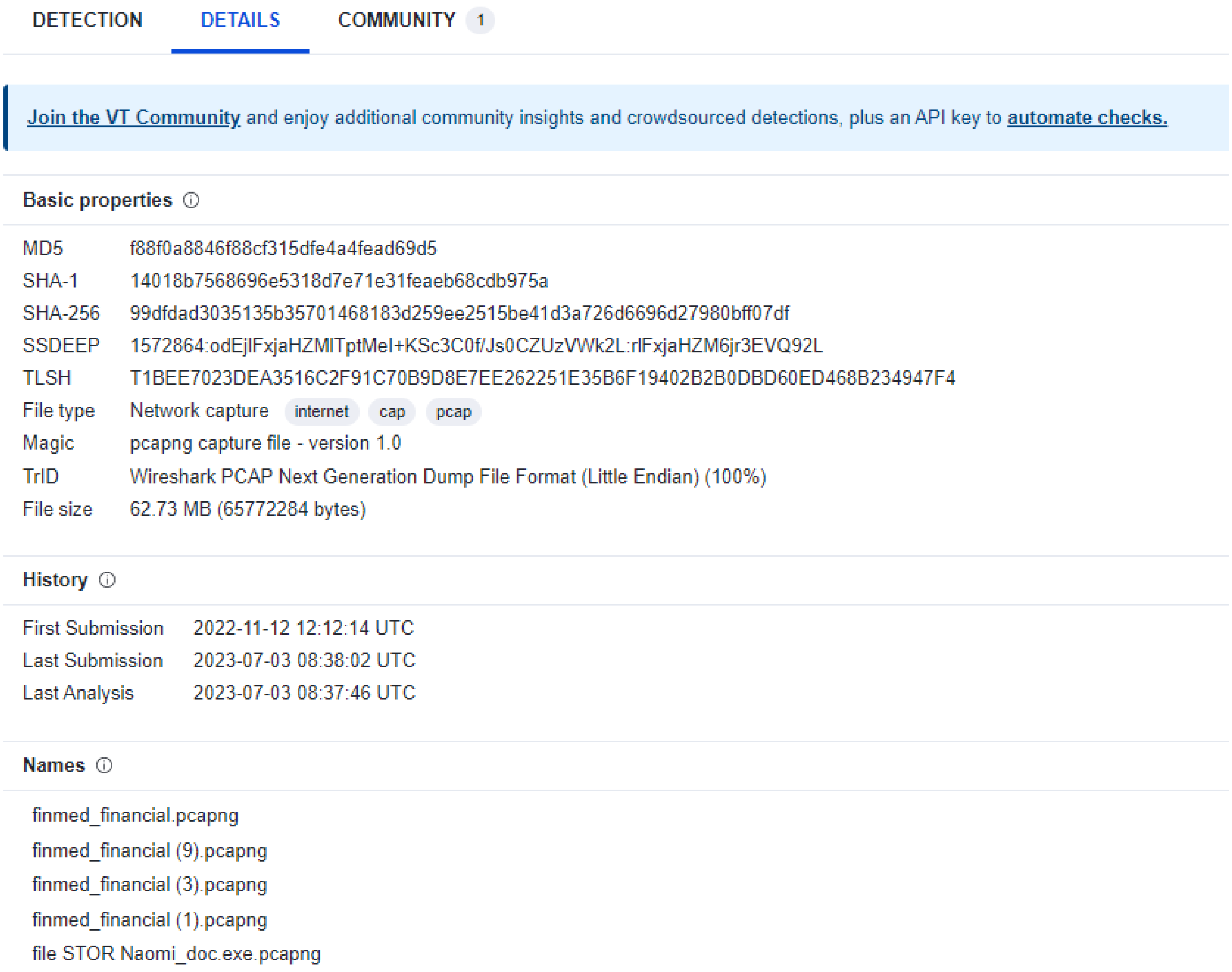
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Cynet	Undetected	Cyren	Undetected
DrWeb	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected

- - In the picture above, the malware check was done on a pcapng file, and 2 malwares were discovered out of 59 distinct files. This prompted me to run another malware test on the.exe file to determine if there was any malware on the server.



Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties ⓘ

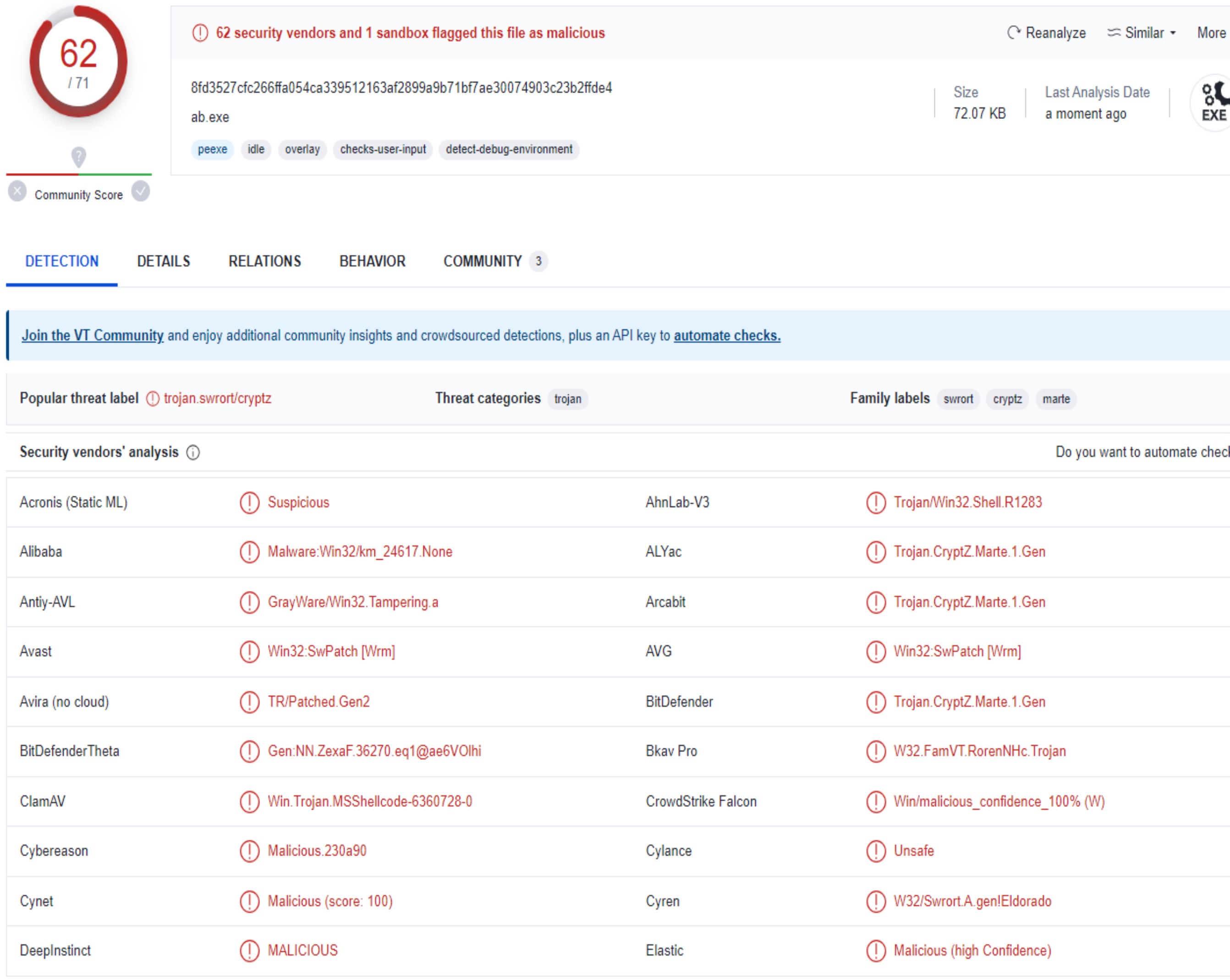
MD5	f88f0a8846f88cf315dfe4a4fead69d5
SHA-1	14018b7568696e5318d7e71e31feaeb68cdb975a
SHA-256	99dfdad3035135b35701468183d259ee2515be41d3a726d6696d27980bff07df
SSDEEP	1572864:odEjlFxjaHZMlTptMel+KSc3C0f/Js0CZUzVWk2L:rlFxjaHZM6jr3EVQ92L
TLSH	T1BEE7023DEA3516C2F91C70B9D8E7EE262251E35B6F19402B2B0DBD60ED468B234947F4
File type	Network capture internet cap pcap
Magic	pcapng capture file - version 1.0
TrID	Wireshark PCAP Next Generation Dump File Format (Little Endian) (100%)
File size	62.73 MB (65772284 bytes)

History ⓘ

First Submission	2022-11-12 12:12:14 UTC
Last Submission	2023-07-03 08:38:02 UTC
Last Analysis	2023-07-03 08:37:46 UTC

Names ⓘ

finmed_financial.pcapng
finmed_financial (9).pcapng
finmed_financial (3).pcapng
finmed_financial (1).pcapng
file STOR Naomi_doc.exe.pcapng



62 security vendors and 1 sandbox flagged this file as malicious

8fd3527cfc266ffa054ca339512163af2899a9b71bf7ae30074903c23b2ffde4

ab.exe

peexe idle overlay checks-user-input detect-debug-environment

Size 72.07 KB

Last Analysis Date a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.swrort/cryptz Threat categories trojan Family labels swrort cryptz marte

Security vendors' analysis

Do you want to automate checl

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32.Shell.R1283
Alibaba	Malware:Win32/km_24617.None	ALYac	Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	GrayWare/Win32.Tampering.a	Arcabit	Trojan.CryptZ.Marte.1.Gen
Avast	Win32:SwPatch [Wrm]	AVG	Win32:SwPatch [Wrm]
Avira (no cloud)	TR/Patched.Gen2	BitDefender	Trojan.CryptZ.Marte.1.Gen
BitDefenderTheta	Gen:NN.ZexaF.36270.eq1@ae6VOlhi	Bkav Pro	W32.FamVT.RorenNHc.Trojan
ClamAV	Win.Trojan.MSShellcode-6360728-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.230a90	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Swrort.A.gen!Eldorado
DeepInstinct	MALICIOUS	Elastic	Malicious (high Confidence)

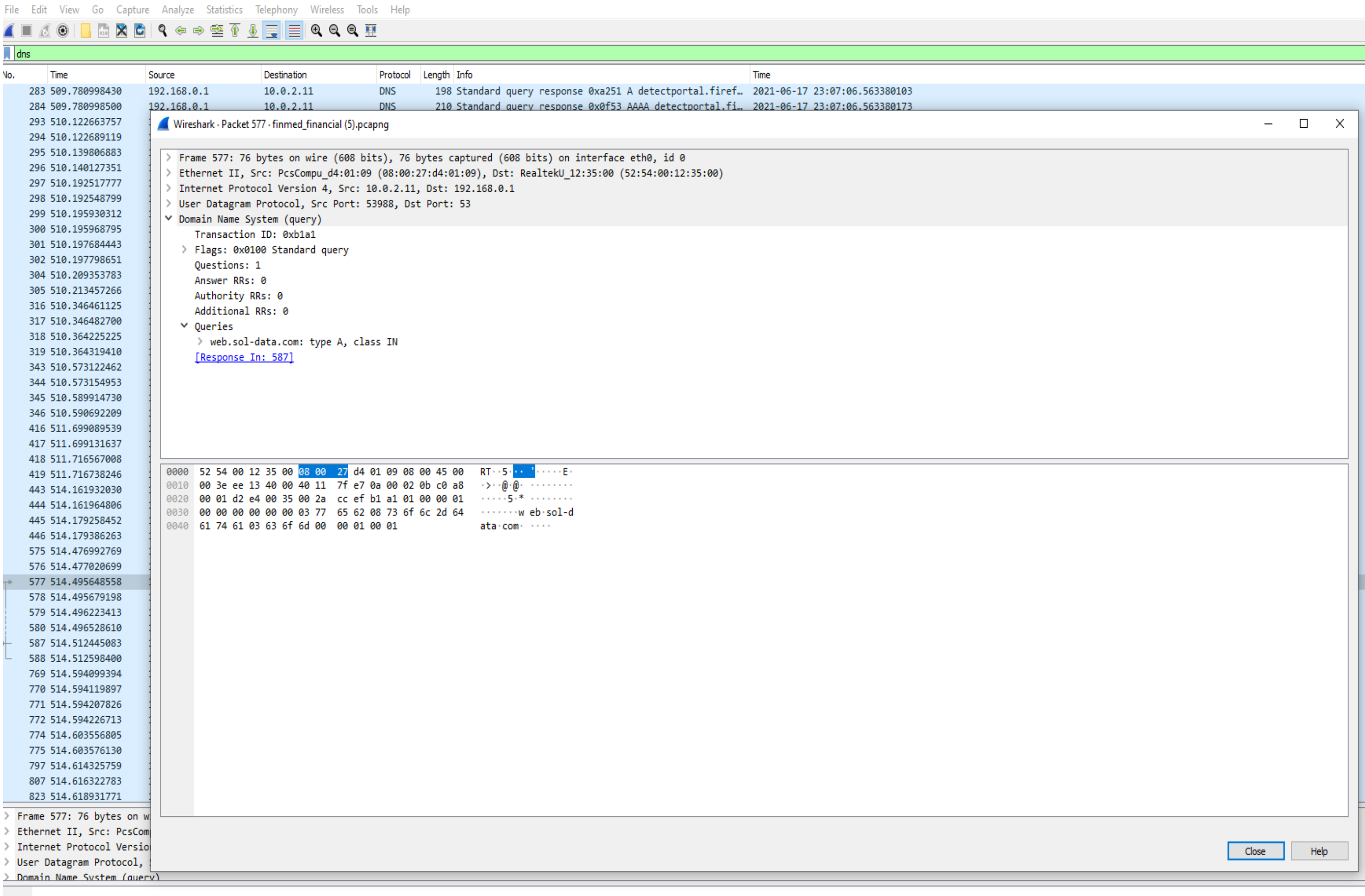
- Malware, short for malicious software, refers to any programme or code designed to harm, exploit, or provide unauthorised access to computer systems, networks, or devices. Malware is a major danger to the security and privacy of consumers, businesses, and organisations since it is created by hackers with malevolent purpose. Malware comes in many forms and is used for a variety of objectives, including viruses, worms, trojans, ransomware, spyware, and botnets.
- In the naomi.exe the maximum malwares were present while I checked on virustotal. The naomi_docs.exe file was uploaded on file server by source IP 10.0.2.16 that belongs to John Corbit. There are definitely large chunks of malware present in the naomi_docs.exe file. The malware file can damage data loss or theft, financial loss, system instability, privacy invasion, unauthorized access, reputational damage, system modification.

DNS Analysis

- The Wireshark network protocol analyzer is used to look at the Domain Name System (DNS) traffic that was recorded in a packet capture file. A fundamental mechanism called DNS is used to convert domain names that can be read by humans, like abc.com, into IP addresses that computers can understand, like 198.0.27.12.

- I have looked through the DNS analysis and went through few websites which are not suspicious or problematic.

DNS

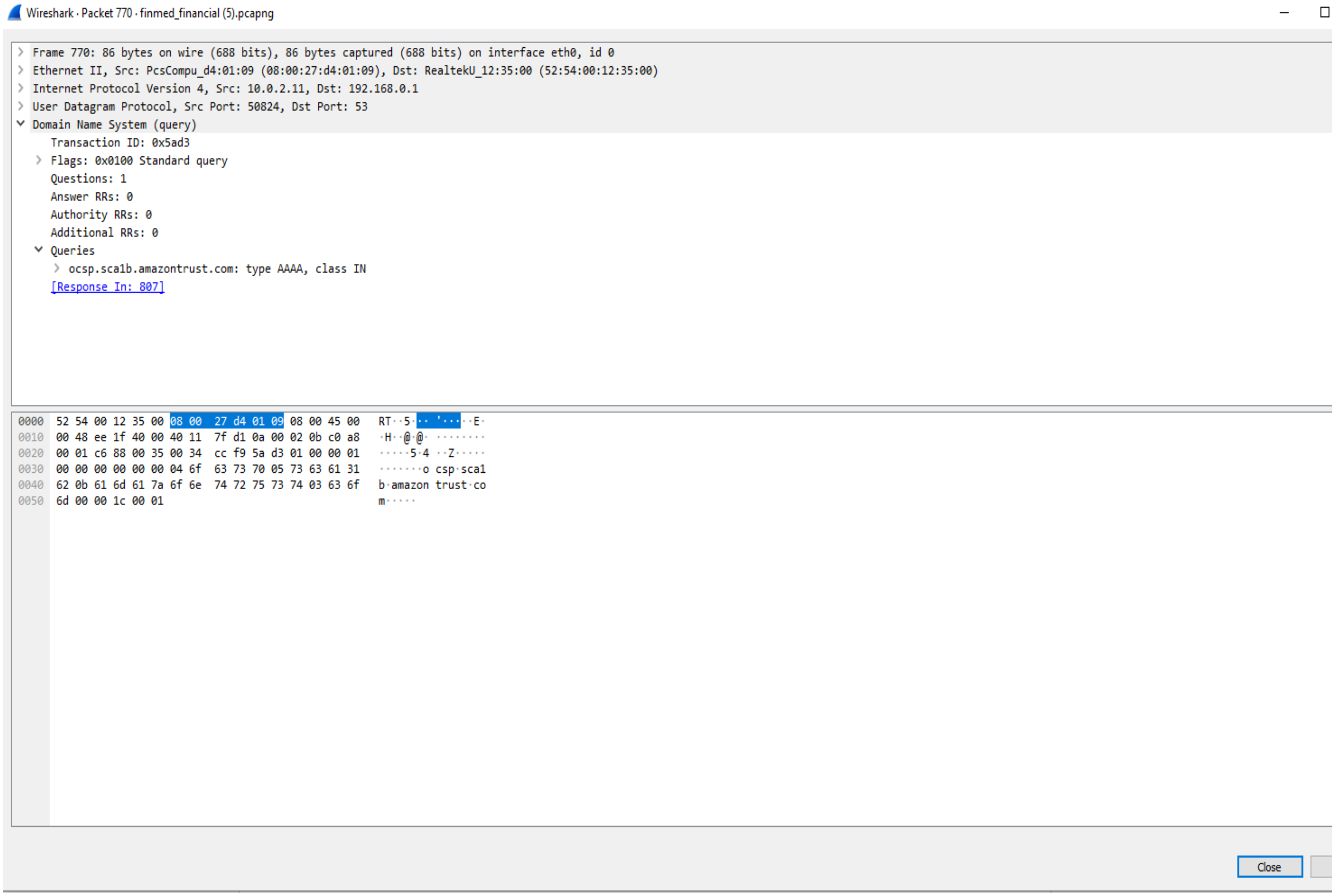


```
No.   Time           Source        Destination  Protocol  Length  Info                                                    Time
  283 509.780998430  192.168.0.1   10.0.2.11    DNS       198 Standard query response 0xa251 A detectportal.firef…  2021-06-17 23:07:06.563380103
  284 509.780998500  192.168.0.1   10.0.2.11    DNS       210 Standard query response 0x0f53 AAAA detectportal.fi…  2021-06-17 23:07:06.563380173
  293 510.122663757
  294 510.122689119
  295 510.139806883
  296 510.140127351
  297 510.192517777
  298 510.192548799
  299 510.195930312
  300 510.195968795
  301 510.197684443
  302 510.197798651
  304 510.209353783
  305 510.213457266
  316 510.346461125
  317 510.346482700
  318 510.364225225
  319 510.364319410
  343 510.573122462
  344 510.573154953
  345 510.589914730
  346 510.590692209
  416 511.699089539
  417 511.699131637
  418 511.716567008
  419 511.716738246
  443 514.161932030
  444 514.161964806
  445 514.179258452
  446 514.179386263
  575 514.476992769
  576 514.477020699
  577 514.495648558
  578 514.495679198
  579 514.496223413
  580 514.496528610
  587 514.512445083
  588 514.512598400
  769 514.594099394
  770 514.594119897
  771 514.594207826
  772 514.594226713
  774 514.603556805
  775 514.603576130
  797 514.614325759
  807 514.616322783
  823 514.618931771
```

```
> Frame 577: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_d4:01:09 (08:00:27:d4:01:09), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.0.2.11, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 53988, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xb1a1
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > web.sol-data.com: type A, class IN
    [Response In: 587]
```

```
0000  52 54 00 12 35 00 08 00  27 d4 01 09 08 00 45 00   RT··5···'·····E·
0010  00 3e ee 13 40 00 40 11  7f e7 0a 00 02 0b c0 a8   ·>··@·@· ········
0020  00 01 d2 e4 00 35 00 2a  cc ef b1 a1 01 00 00 01   ·····5·* ········
0030  00 00 00 00 00 00 03 77  65 62 08 73 6f 6c 2d 64   ·······w eb·sol-d
0040  61 74 61 03 63 6f 6d 00  00 01 00 01               ata·com· ····
```

```
> Frame 577: 76 bytes on w
> Ethernet II, Src: PcsCom
> Internet Protocol Versio
> User Datagram Protocol,
> Domain Name System (query)
```

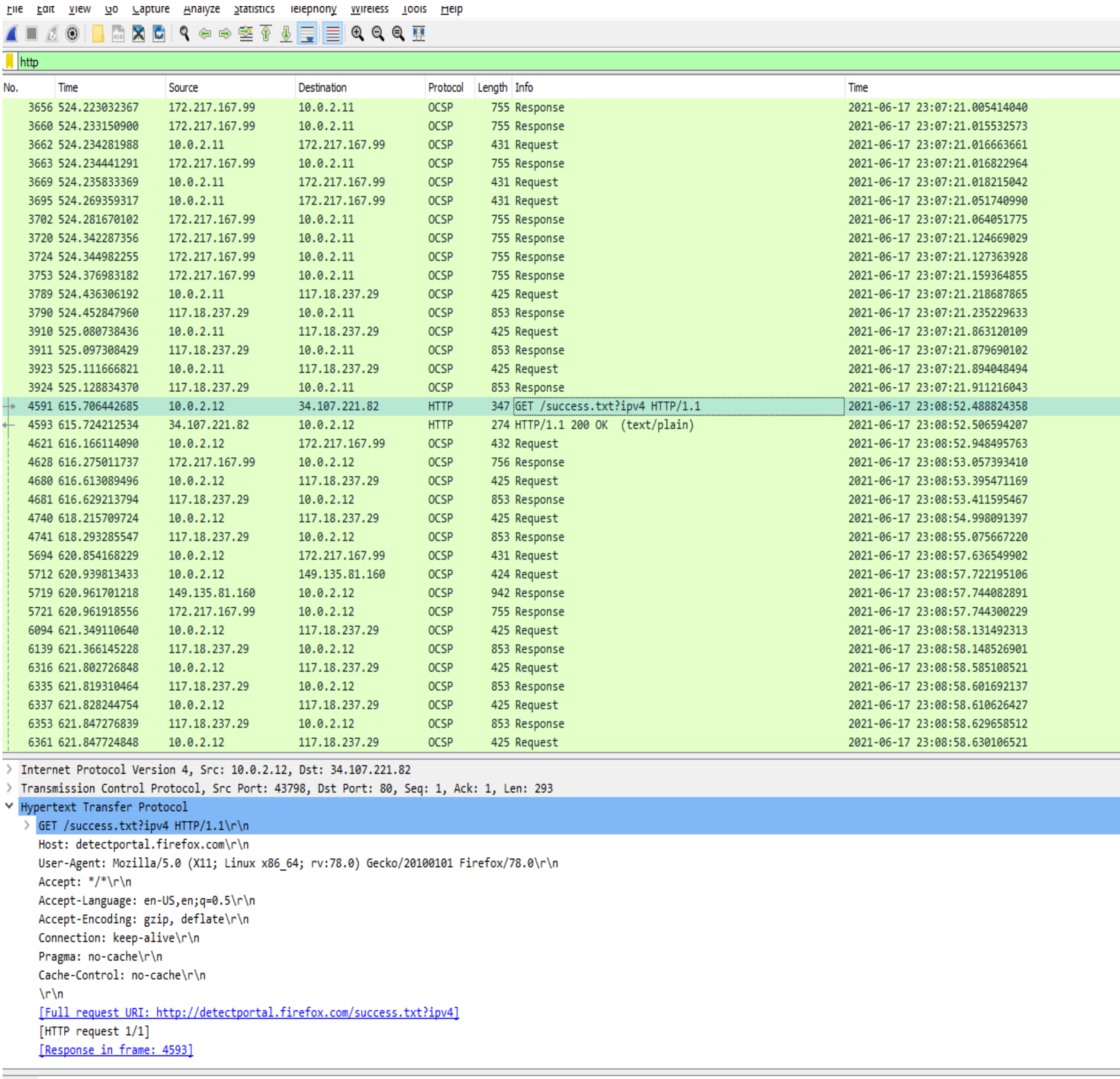


```
> Frame 770: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_d4:01:09 (08:00:27:d4:01:09), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.0.2.11, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 50824, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x5ad3
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > ocsp.sca1b.amazontrust.com: type AAAA, class IN
    [Response In: 807]
```

```
0000  52 54 00 12 35 00 08 00  27 d4 01 09 08 00 45 00   RT··5··· '·····E·
0010  00 48 ee 1f 40 00 40 11  7f d1 0a 00 02 0b c0 a8   ·H··@·@· ········
0020  00 01 c6 88 00 35 00 34  cc f9 5a d3 01 00 00 01   ·····5·4 ··Z·····
0030  00 00 00 00 00 00 04 6f  63 73 70 05 73 63 61 31   ·······o csp·sca1
0040  62 0b 61 6d 61 7a 6f 6e  74 72 75 73 74 03 63 6f   b·amazon trust·co
0050  6d 00 00 1c 00 01                                  m·····
```

HTTP Analysis

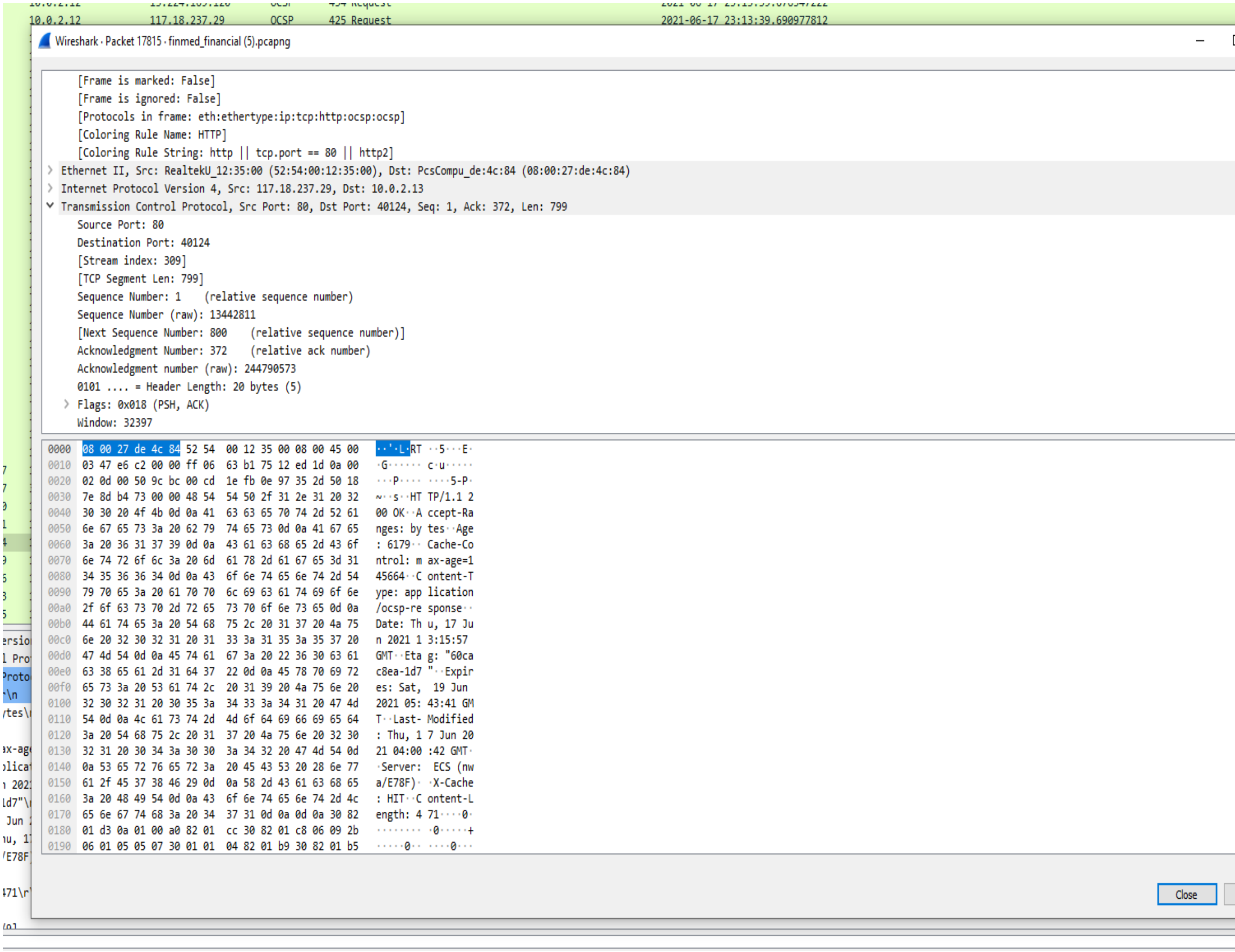
The HTTP analysis of the incident reveals some information on how the virus got into the FTP server. The virus was uploaded using a POST request, which implies the attacker submitted it to the server as part of a form. This shows that the attacker may have duped a member of staff into submitting the virus to the server by sending them a malicious link or email. The incident's HTTP analysis also reveals some information about the sort of malware that was uploaded to the FTP site. The software was a Trojan horse built to steal user credentials. This shows that the attacker was attempting to obtain access to the user accounts of Finmed Financial Fusion employees. Investigators might benefit from the HTTP analysis of the occurrence. It can aid in determining the mechanism used to introduce the virus to the server, the sort of malware that was uploaded, and the attacker's objectives. This information may be utilized to devise a strategy to reduce the likelihood of future assaults and to hunt down the perpetrator.



```
http
```

```
No.   Time           Source          Destination     Protocol Length Info                                    Time
 3656 524.223032367  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.005414040
 3660 524.233150900  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.015532573
 3662 524.234281988  10.0.2.11       172.217.167.99  OCSP     431 Request                                    2021-06-17 23:07:21.016663661
 3663 524.234441291  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.016822964
 3669 524.235833369  10.0.2.11       172.217.167.99  OCSP     431 Request                                    2021-06-17 23:07:21.018215042
 3695 524.269359317  10.0.2.11       172.217.167.99  OCSP     431 Request                                    2021-06-17 23:07:21.051740990
 3702 524.281670102  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.064051775
 3720 524.342287356  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.124669029
 3724 524.344982255  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.127363928
 3753 524.376983182  172.217.167.99  10.0.2.11       OCSP     755 Response                                   2021-06-17 23:07:21.159364855
 3789 524.436306192  10.0.2.11       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:07:21.218687865
 3790 524.452847960  117.18.237.29   10.0.2.11       OCSP     853 Response                                   2021-06-17 23:07:21.235229633
 3910 525.080738436  10.0.2.11       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:07:21.863120109
 3911 525.097308429  117.18.237.29   10.0.2.11       OCSP     853 Response                                   2021-06-17 23:07:21.879690102
 3923 525.111666821  10.0.2.11       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:07:21.894048494
 3924 525.128834370  117.18.237.29   10.0.2.11       OCSP     853 Response                                   2021-06-17 23:07:21.911216043
 4591 615.706442685  10.0.2.12       34.107.221.82   HTTP     347 GET /success.txt?ipv4 HTTP/1.1             2021-06-17 23:08:52.488824358
 4593 615.724212534  34.107.221.82   10.0.2.12       HTTP     274 HTTP/1.1 200 OK  (text/plain)              2021-06-17 23:08:52.506594207
 4621 616.166114090  10.0.2.12       172.217.167.99  OCSP     432 Request                                    2021-06-17 23:08:52.948495763
 4628 616.275011737  172.217.167.99  10.0.2.12       OCSP     756 Response                                   2021-06-17 23:08:53.057393410
 4680 616.613089496  10.0.2.12       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:08:53.395471169
 4681 616.629213794  117.18.237.29   10.0.2.12       OCSP     853 Response                                   2021-06-17 23:08:53.411595467
 4740 618.215709724  10.0.2.12       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:08:54.998091397
 4741 618.293285547  117.18.237.29   10.0.2.12       OCSP     853 Response                                   2021-06-17 23:08:55.075667220
 5694 620.854168229  10.0.2.12       172.217.167.99  OCSP     431 Request                                    2021-06-17 23:08:57.636549902
 5712 620.939813433  10.0.2.12       149.135.81.160  OCSP     424 Request                                    2021-06-17 23:08:57.722195106
 5719 620.961701218  149.135.81.160  10.0.2.12       OCSP     942 Response                                   2021-06-17 23:08:57.744082891
 5721 620.961918556  172.217.167.99  10.0.2.12       OCSP     755 Response                                   2021-06-17 23:08:57.744300229
 6094 621.349110640  10.0.2.12       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:08:58.131492313
 6139 621.366145228  117.18.237.29   10.0.2.12       OCSP     853 Response                                   2021-06-17 23:08:58.148526901
 6316 621.802726848  10.0.2.12       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:08:58.585108521
 6335 621.819310464  117.18.237.29   10.0.2.12       OCSP     853 Response                                   2021-06-17 23:08:58.601692137
 6337 621.828244754  10.0.2.12       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:08:58.610626427
 6353 621.847276839  117.18.237.29   10.0.2.12       OCSP     853 Response                                   2021-06-17 23:08:58.629658512
 6361 621.847724848  10.0.2.12       117.18.237.29   OCSP     425 Request                                    2021-06-17 23:08:58.630106521
```

```
> Internet Protocol Version 4, Src: 10.0.2.12, Dst: 34.107.221.82
> Transmission Control Protocol, Src Port: 43798, Dst Port: 80, Seq: 1, Ack: 1, Len: 293
v Hypertext Transfer Protocol
  > GET /success.txt?ipv4 HTTP/1.1\r\n
    Host: detectportal.firefox.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://detectportal.firefox.com/success.txt?ipv4]
    [HTTP request 1/1]
    [Response in frame: 4593]
```

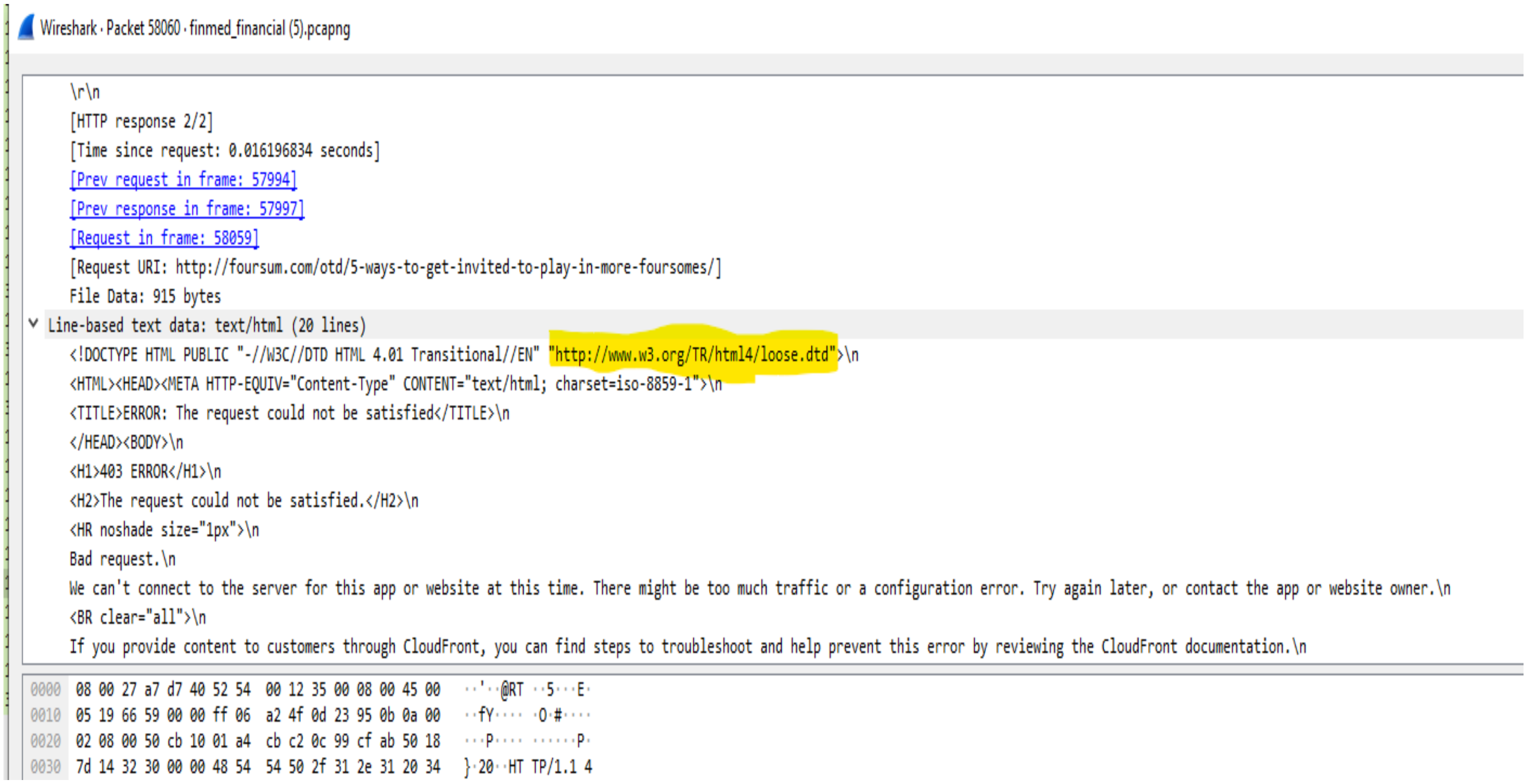


```
10.0.2.12        117.18.237.29    OCSP    425 Request                                2021-06-17 23:13:39.690977812
```

Wireshark · Packet 17815 · finmed_financial (5).pcapng

```
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:ocsp:ocsp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_de:4c:84 (08:00:27:de:4c:84)
> Internet Protocol Version 4, Src: 117.18.237.29, Dst: 10.0.2.13
v Transmission Control Protocol, Src Port: 80, Dst Port: 40124, Seq: 1, Ack: 372, Len: 799
    Source Port: 80
    Destination Port: 40124
    [Stream index: 309]
    [TCP Segment Len: 799]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 13442811
    [Next Sequence Number: 800    (relative sequence number)]
    Acknowledgment Number: 372    (relative ack number)
    Acknowledgment number (raw): 244790573
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 32397
```

```
0000  08 00 27 de 4c 84 52 54  00 12 35 00 08 00 45 00   ··'·L·RT ··5···E·
0010  03 47 e6 c2 00 00 ff 06  63 b1 75 12 ed 1d 0a 00   ·G······ c·u·····
0020  02 0d 00 50 9c bc 00 cd  1e fb 0e 97 35 2d 50 18   ···P···· ····5-P·
0030  7e 8d b4 73 00 00 48 54  54 50 2f 31 2e 31 20 32   ~··s··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 41  63 63 65 70 74 2d 52 61   00 OK··A ccept-Ra
0050  6e 67 65 73 3a 20 62 79  74 65 73 0d 0a 41 67 65   nges: by tes··Age
0060  3a 20 36 31 37 39 0d 0a  43 61 63 68 65 2d 43 6f   : 6179·· Cache-Co
0070  6e 74 72 6f 6c 3a 20 6d  61 78 2d 61 67 65 3d 31   ntrol: m ax-age=1
0080  34 35 36 36 34 0d 0a 43  6f 6e 74 65 6e 74 2d 54   45664··C ontent-T
0090  79 70 65 3a 20 61 70 70  6c 69 63 61 74 69 6f 6e   ype: app lication
00a0  2f 6f 63 73 70 2d 72 65  73 70 6f 6e 73 65 0d 0a   /ocsp-re sponse··
00b0  44 61 74 65 3a 20 54 68  75 2c 20 31 37 20 4a 75   Date: Th u, 17 Ju
00c0  6e 20 32 30 32 31 20 31  33 3a 31 35 3a 35 37 20   n 2021 1 3:15:57 
00d0  47 4d 54 0d 0a 45 74 61  67 3a 20 22 36 30 63 61   GMT··Eta g: "60ca
00e0  63 38 65 61 2d 31 64 37  22 0d 0a 45 78 70 69 72   c8ea-1d7 "··Expir
00f0  65 73 3a 20 53 61 74 2c  20 31 39 20 4a 75 6e 20   es: Sat,  19 Jun 
0100  32 30 32 31 20 30 35 3a  34 33 3a 34 31 20 47 4d   2021 05: 43:41 GM
0110  54 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   T··Last- Modified
0120  3a 20 54 68 75 2c 20 31  37 20 4a 75 6e 20 32 30   : Thu, 1 7 Jun 20
0130  32 31 20 30 34 3a 30 30  3a 34 32 20 47 4d 54 0d   21 04:00 :42 GMT·
0140  0a 53 65 72 76 65 72 3a  20 45 43 53 20 28 6e 77   ·Server:  ECS (nw
0150  61 2f 45 37 38 46 29 0d  0a 58 2d 43 61 63 68 65   a/E78F)· ·X-Cache
0160  3a 20 48 49 54 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   : HIT··C ontent-L
0170  65 6e 67 74 68 3a 20 34  37 31 0d 0a 0d 0a 30 82   ength: 4 71····0·
0180  01 d3 0a 01 00 a0 82 01  cc 30 82 01 c8 06 09 2b   ········ ·0·····+
0190  06 01 05 05 07 30 01 01  04 82 01 b9 30 82 01 b5   ·····0·· ····0···
```



Wireshark · Packet 58060 · finmed_financial (5).pcapng

```
        \r\n
        [HTTP response 2/2]
        [Time since request: 0.016196834 seconds]
        [Prev request in frame: 57994]
        [Prev response in frame: 57997]
        [Request in frame: 58059]
        [Request URI: http://foursum.com/otd/5-ways-to-get-invited-to-play-in-more-foursomes/]
        File Data: 915 bytes
  v Line-based text data: text/html (20 lines)
        <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">\n
        <HTML><HEAD><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">\n
        <TITLE>ERROR: The request could not be satisfied</TITLE>\n
        </HEAD><BODY>\n
        <H1>403 ERROR</H1>\n
        <H2>The request could not be satisfied.</H2>\n
        <HR noshade size="1px">\n
        Bad request.\n
        We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner.\n
        <BR clear="all">\n
        If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.\n

0000  08 00 27 a7 d7 40 52 54  00 12 35 00 08 00 45 00   ··'··@RT ··5···E·
0010  05 19 66 59 00 00 ff 06  a2 4f 0d 23 95 0b 0a 00   ··fY···· ·O·#····
0020  02 08 00 50 cb 10 01 a4  cb c2 0c 99 cf ab 50 18   ···P···· ······P·
0030  7d 14 32 30 00 00 48 54  54 50 2f 31 2e 31 20 34   }·20··HT TP/1.1 4
```

Conclusion

Finally, the Finmed Financial Fusion cybersecurity incident investigation has given light on a probable malware file located on the FTP server. We acquired useful insights into the nature and effect of the incident, as well as its likely relation to internal staff issues, through a detailed examination of the occurrence and the accompanying pcap file. The discovery of a suspected malware file on the FTP server emphasizes how vital it is to have a strong and proactive cybersecurity posture. The event exposed existing security flaws and vulnerabilities in our network architecture, emphasizing the importance of taking urgent action to fortify our defenses and safeguard critical data.

Finmed Financial Fusion was the target of a possible malware assault. However, I believe that the actions I've suggested will assist in reducing the likelihood of future assaults. I strongly encourage the bank to put these suggestions into action as quickly as feasible.

Finmed Financial Fusion should consider taking the following security measures in addition to the actions indicated above:

- To prevent sensitive data from being exfiltrated from the network, use a data loss prevention (DLP) solution.
- To find and repair security flaws, implement a vulnerability management program.
- Create a disaster recovery strategy to guarantee that your company can continue to operate in the case of a cyberattack.

Finmed Financial Fusion may strengthen its overall security posture and lower the risk of cybercrime by following these actions.

References

Academy, A 2017, *DNS Protocol*, viewed October 2020, <https://www.youtube.com/watch?v=FWwgVKlxxGM&list=PLEitx5IL8YVwyieWkraVJ1Q99CE84P2BA&index=14>.

Aguilar, J 2018, *Mastering Wireshark 2 : UDP Analysis*, viewed October 26, <https://www.youtube.com/watch?v=afO7hGrYIc0>.

CertBros 2020, *TCP vs UDP Comparison | Cisco CCNA 200-301*, viewed October 26, <https://www.youtube.com/watch?v=cA9ZJdqzOoU>.

Cisco 2016, *TCP and UDP: Comparing Transport Protocols*, viewed October 26, <https://www.youtube.com/watch?v=MMDhvHYAF7E>.

Computer, DP 2014, *TCP, UDP, and Ports*, D Pro Computer, viewed October, <https://www.youtube.com/watch?v=FpZmTJNIMZI>.

Explained, B 2016, *WireShark : Capture Filters Exercise ICMP & HTTP*, viewed October 26, <https://www.youtube.com/watch?v=z8-aXaDq43M>.

Ghosh, B 2019, *OSI Network Layer Analysis via Wireshark*, viewed October 26, <https://linuxhint.com/osi_network_layer_analsysis_wireshark/>.

Graziani, R 2018, *TCP: Terminating the Connection*, viewed October 26, <https://www.youtube.com/watch?v=bKQfbkE1Nac>.