Executive Summary

In analyzing the PCAP file, the employee we're investigating first logged on and used google to search for 'fire tornados.' They then downloaded some FireFox browser documentation files, before visiting a gaming site 'zeemud.org.' While no definitive evidence of malicious activity was found, we should consider if this employee might have violated the corporate Acceptable Use Policy.

Technical Appendix

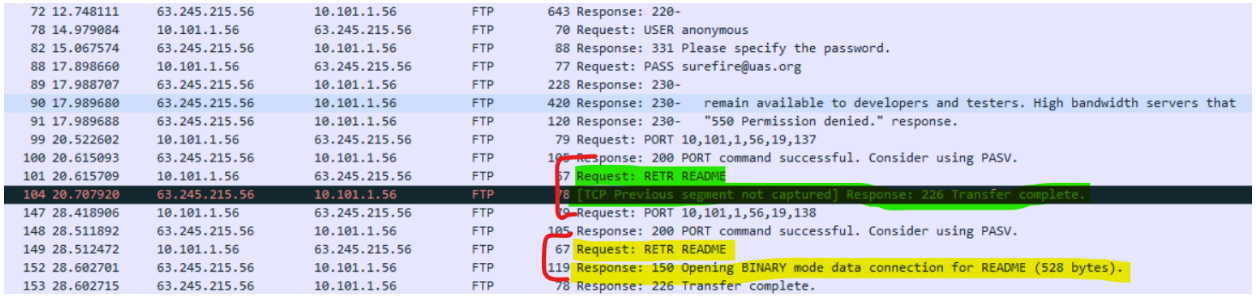
WireShark Investigation:

Active Hypotheses:

It does appear that the employee visited google, searched for 'fire tornado', downloaded some sort of documentation files, and then proceeded to visit the gaming site 'zeemud.org.'

It looks like the employee interacted with the following servers: 63.245.215.56 | 74.125.225.101 | 74.125.225.180 | 209.128.72.218.

They did not upload any files, but they did download files. The first download attempt seemed to have a packet capture related issue, but the second went through without issue (screenshot below).



72	12.748111	63.245.215.56	10.101.1.56	FTP	643 Response: 220-
78	14.979084	10.101.1.56	63.245.215.56	FTP	70 Request: USER anonymous
82	15.067574	63.245.215.56	10.101.1.56	FTP	88 Response: 331 Please specify the password.
88	17.898660	10.101.1.56	63.245.215.56	FTP	77 Request: PASS surefire@uas.org
89	17.988707	63.245.215.56	10.101.1.56	FTP	228 Response: 230-
90	17.989680	63.245.215.56	10.101.1.56	FTP	420 Response: 230- remain available to developers and testers. High bandwidth servers that
91	17.989688	63.245.215.56	10.101.1.56	FTP	120 Response: 230- "550 Permission denied." response.
99	20.522602	10.101.1.56	63.245.215.56	FTP	79 Request: PORT 10,101,1,56,19,137
100	20.615093	63.245.215.56	10.101.1.56	FTP	105 Response: 200 PORT command successful. Consider using PASV.
101	20.615709	10.101.1.56	63.245.215.56	FTP	67 Request: RETR README
104	20.707920	63.245.215.56	10.101.1.56	FTP	78 [TCP Previous segment not captured] Response: 226 Transfer complete.
147	28.418906	10.101.1.56	63.245.215.56	FTP	79 Request: PORT 10,101,1,56,19,138
148	28.511892	63.245.215.56	10.101.1.56	FTP	105 Response: 200 PORT command successful. Consider using PASV.
149	28.512472	10.101.1.56	63.245.215.56	FTP	67 Request: RETR README
152	28.602701	63.245.215.56	10.101.1.56	FTP	119 Response: 150 Opening BINARY mode data connection for README (528 bytes).
153	28.602715	63.245.215.56	10.101.1.56	FTP	78 Response: 226 Transfer complete.

Regarding the “weird text” - I believe it’s possible that this is what the employee was referring to:

```
File Transfer Protocol (FTP)
> 220-\r\n
  220-   ftp.mozilla.org / archive.mozilla.org - files are in /pub/mozilla.org\r\n
  220-\r\n
  220-   Notice: This server is the only place to obtain nightly builds and needs to\r\n
  220-   remain available to developers and testers. High bandwidth servers that\r\n
  220-   contain the public release files are available at ftp://releases.mozilla.org/\r\n
  220-   If you need to link to a public release, please link to the release server,\r\n
  220-   not here. Thanks!\r\n
  220-\r\n
  220-   Attempts to download high traffic release files from this server will get a\r\n
  220-   "550 Permission denied." response.\r\n
  220 \r\n
```

The above was displayed under the expanded Packet Details for No.72 (below). We can see the destination IP was the employee’s device (10.101.1.56).

72	12.748111	63.245.215.56	10.101.1.56	FTP	643 Response: 220-

Verified Facts:

The employee visited the following sites: google.com, download.com, mozilla.org, & zeemud.org (screenshot below):

34	5.037126	10.101.1.56	75.75.76.76	DNS	79 Standard query 0x9b0a A clients1.google.com
35	5.074614	75.75.76.76	10.101.1.56	DNS	279 Standard query response 0x9b0a A clients1.google.com CNAME clients.l.google.com A 74.125.225.101 A 74.125.225.97 A 74.125.225.102 A…
45	6.839648	10.101.1.56	75.75.76.76	DNS	76 Standard query 0x590b A ftp.download.com
46	6.951377	75.75.76.76	10.101.1.56	DNS	132 Standard query response 0x590b A ftp.download.com CNAME phx1-sha-redirect-lb.cnet.com A 64.30.224.118
67	12.441535	10.101.1.56	75.75.76.76	DNS	75 Standard query 0xf599 A ftp.mozilla.org
68	12.566457	75.75.76.76	10.101.1.56	DNS	171 Standard query response 0xf599 A ftp.mozilla.org CNAME ftp.dynect.mozilla.net CNAME ftp2-zlb.vips.scl3.mozilla.com A 63.245.215.56
122	24.238864	10.101.1.56	75.75.76.76	DNS	74 Standard query 0xbca6 A mud.zeemud.org
123	24.486097	75.75.76.76	10.101.1.56	DNS	104 Standard query response 0xbca6 A mud.zeemud.org CNAME zeemud.org A 209.128.72.218

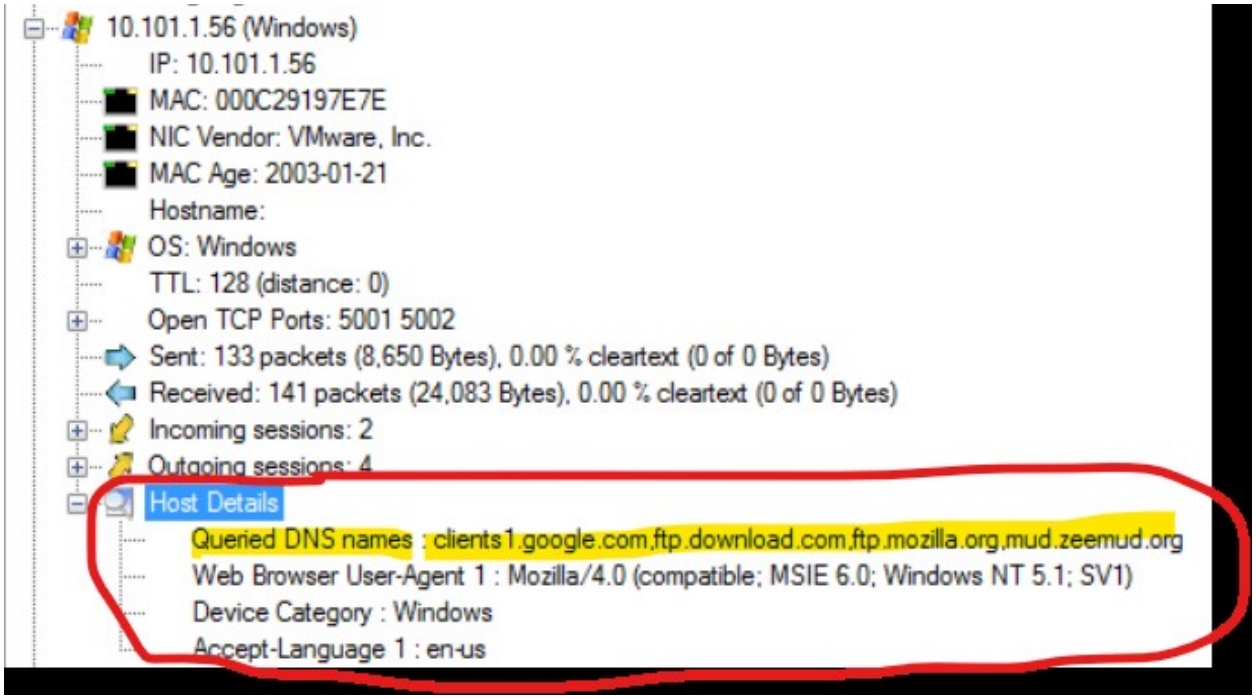
NetworkMiner Investigation:

Active Hypotheses:

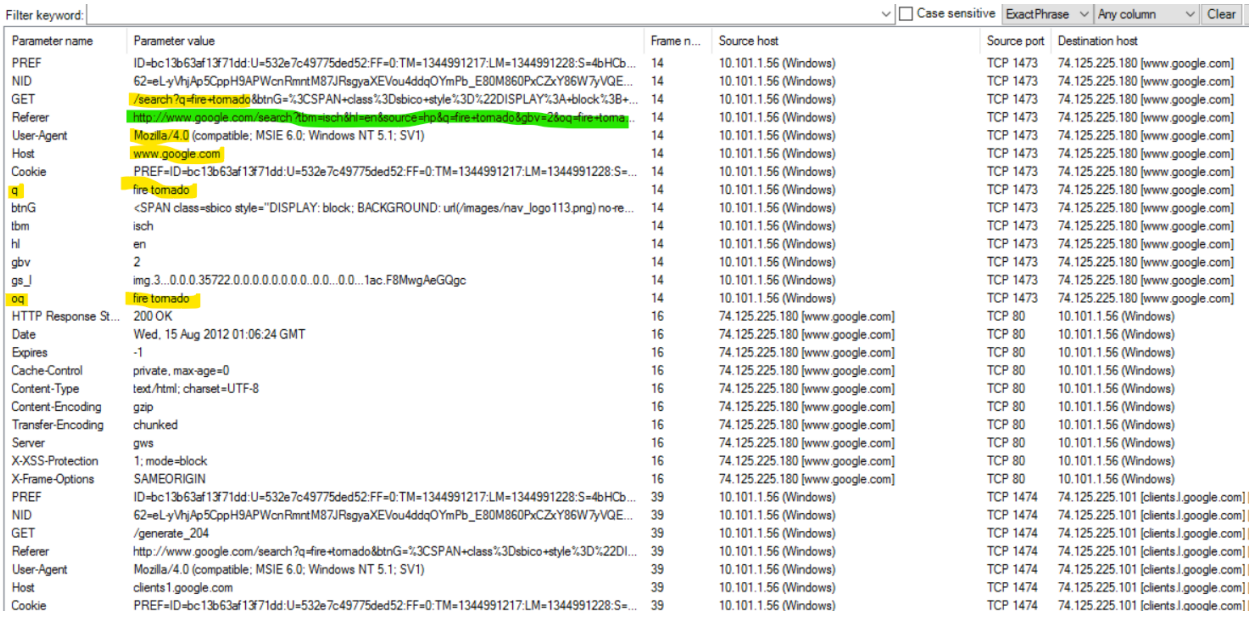
Employee got online, opened up a Mozilla Firefox browser, went to google, searched 'fire tornado', downloaded a few files and visited 'zeemud.org' (what appears to be a game site).

Employee IP: 10.101.1.56

It looks like the employee visited the following (4) servers: 63.245.215.56 | 74.125.225.101 | 74.125.225.180 | 209.128.72.218; and the following sites: google.com (clients.l.google.com), ftp.download.com/ftp.mozilla.org/ftp.dynect.mozilla.net, zeemud.org (mud.zeemud.org). We can see all this in the screenshot below:



From the Parameters tab (screenshot below), we can see the google search the employee made (green), and that full google query was for 'fire tornado' - the full path is here (safe to click on - is just a google search).



Filter keyword: Case sensitive ExactPhrase Any column Clear

Parameter name	Parameter value	Frame n...	Source host	Source port	Destination host
PREF	ID=bc13b63af13f71dd:U=532e7c49775ded52:FF=0:TM=1344991217:LM=1344991228:S=4bHCb...	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
NID	62=eL-yVhjAp5CppH9APWcnRmntM87JRsgyaXEVou4ddqOYmPb_E80M860PxCZxY86W7yVQE...	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
GET	/search?q=fire+tomado&btnG=%3CSPAN+class%3Dsbico+style%3D%22DISPLAY%3A+block%3B+...	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
Referer	http://www.google.com/search?tbm=isch&hl=en&source=hp&q=fire+tomado&gbv=2&oq=fire+toma...	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
Host	www.google.com	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
Cookie	PREF=ID=bc13b63af13f71dd:U=532e7c49775ded52:FF=0:TM=1344991217:LM=1344991228:S=...	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
q	fire tomado	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
btnG	<SPAN class=sbico style="DISPLAY: block; BACKGROUND: url(/images/nav_logo113.png) no-re...	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
tbm	isch	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
hl	en	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
gbv	2	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
gs_l	img.3...0.0.0.35722.0.0.0.0.0.0.0.0..0.0...0.0...1ac.F8MwgAeGQgc	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
oq	fire tomado	14	10.101.1.56 (Windows)	TCP 1473	74.125.225.180 [www.google.com]
HTTP Response St...	200 OK	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Date	Wed, 15 Aug 2012 01:06:24 GMT	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Expires	-1	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Cache-Control	private, max-age=0	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Content-Type	text/html; charset=UTF-8	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Content-Encoding	gzip	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Transfer-Encoding	chunked	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
Server	gws	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
X-XSS-Protection	1; mode=block	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
X-Frame-Options	SAMEORIGIN	16	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)
PREF	ID=bc13b63af13f71dd:U=532e7c49775ded52:FF=0:TM=1344991217:LM=1344991228:S=4bHCb...	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]
NID	62=eL-yVhjAp5CppH9APWcnRmntM87JRsgyaXEVou4ddqOYmPb_E80M860PxCZxY86W7yVQE...	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]
GET	/generate_204	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]
Referer	http://www.google.com/search?q=fire+tomado&btnG=%3CSPAN+class%3Dsbico+style%3D%22DI...	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]
User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]
Host	clients1.google.com	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]
Cookie	PREF=ID=bc13b63af13f71dd:U=532e7c49775ded52:FF=0:TM=1344991217:LM=1344991228:S=...	39	10.101.1.56 (Windows)	TCP 1474	74.125.225.101 [clients1.google.com]

The following screenshot contains the timestamps from beginning (yellow) to end (blue) with the corresponding client/server host requests and sites visited (green). This shows the beginning where the employee put in a request to visit google.com, made several additional requests in google, and was redirected to a few different sites afterward.

Frame nr.	Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:00:56	0x9B0A	0x0005 (CNAME)	clients1.google.com	clients.l.google.com
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.101
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.97
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.102
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.105
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.96
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.103
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.98
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.104
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.110
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.99
35	2012-08-15 01:06:28 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:02:45	0x9B0A	0x0001 (A)	clients.l.google.com	74.125.225.100
46	2012-08-15 01:06:30 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:05:00	0x590B	0x0005 (CNAME)	ftp.download.com	phx1-sha-redirect-lb.cnet.com
46	2012-08-15 01:06:30 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:01:26	0x590B	0x0001 (A)	phx1-sha-redirect-lb.cnet.com	64.30.224.118
68	2012-08-15 01:06:35 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:03:59	0xF599	0x0005 (CNAME)	ftp.mozilla.org	ftp.dynect.mozilla.net
68	2012-08-15 01:06:35 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:00:30	0xF599	0x0005 (CNAME)	ftp.dynect.mozilla.net	ftp2-zlb.vips.scl3.mozilla.com
68	2012-08-15 01:06:35 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	00:05:00	0xF599	0x0001 (A)	ftp2-zlb.vips.scl3.mozilla.com	63.245.215.56
123	2012-08-15 01:06:47 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	02:00:00	0xBCA6	0x0005 (CNAME)	mud.zeemud.org	zeemud.org
123	2012-08-15 01:06:47 UTC	10.101.1.56 (Windows)	1305	75.75.76.76	53	53	02:00:00	0xBCA6	0x0001 (A)	zeemud.org	209.128.72.218

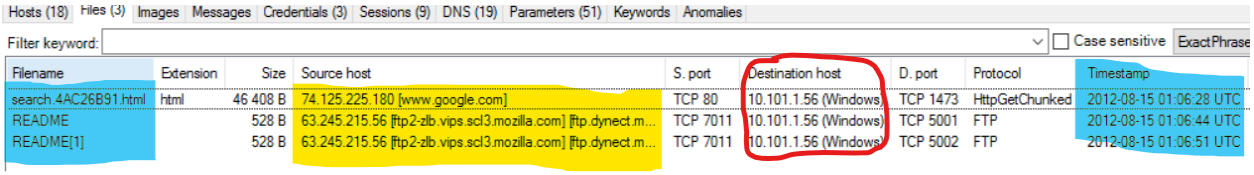
Verified Facts:

- *IP of employee is 10.101.1.56
- *Employee OS was Windows
- *The employee queried the following DNS names :
clients1.google.com,ftp.download.com,ftp.mozilla.org,mud.zeemud.org

*these were confirmed and moved to verified facts from active hypotheses

- Zeemud.org - upon further inspection, is a site that hosts a “swords and sorcery themed” text-based role-playing game.

(3) total files were downloaded: 1 from Google, and 2 through Mozilla hosts.



Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
search.4AC26B91.html	html	46 408 B	74.125.225.180 [www.google.com]	TCP 80	10.101.1.56 (Windows)	TCP 1473	HttpGetChunked	2012-08-15 01:06:28 UTC
README		528 B	63.245.215.56 [ftp2-zlb.vips.scl3.mozilla.com] [ftp.dynect.m...	TCP 7011	10.101.1.56 (Windows)	TCP 5001	FTP	2012-08-15 01:06:44 UTC
README[1]		528 B	63.245.215.56 [ftp2-zlb.vips.scl3.mozilla.com] [ftp.dynect.m...	TCP 7011	10.101.1.56 (Windows)	TCP 5002	FTP	2012-08-15 01:06:51 UTC

Self-Directed Learning

WireShark Investigation

Open Questions:

WireShark Default Coloring Rules Table

Name	Filter
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
ARP	arp
ICMP	icmp || icmpv6
TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp || carp))
Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sctp.checksum.status=="Bad" ||
SMB	smb || nbss || nbns || netbios
HTTP	http || tcp.port == 80 || http2
DCERPC	dcerpc
Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1
System Event	systemd_journal || sysdig

Bad TCP: The 'Bad TCP' coloring rule can be triggered by various TCP-related issues, such as:

TCP checksum errors: If the TCP checksum calculation does not match the expected value, it suggests that there may be data corruption or transmission errors.

Out-of-order packets: If the TCP packets are received out of order, it can indicate issues with packet reordering, network congestion, or misconfigurations.

Retransmissions: When Wireshark detects duplicate TCP packets or packets that are being retransmitted, it may apply the 'Bad tcp' coloring rule to highlight potential performance or reliability issues.

TCP protocol violations: If a TCP packet violates the TCP protocol specifications, such as incorrect sequence numbers, invalid flags, or unexpected TCP options, Wireshark may flag it as 'Bad tcp'.

TCP RST: The TCP RST flag is a control flag used in TCP communication to reset a TCP connection. When a TCP RST packet is sent, it indicates an immediate termination or reset of the connection. This can occur for various reasons, such as when a host receives a TCP packet for a connection that does not exist or when a host wants to abruptly terminate an established TCP connection.

SCTP ABORT: refers to the default coloring rule applied to packets that belong to the SCTP (Stream Control Transmission Protocol) and contain the SCTP ABORT chunk.

SCTP is a transport layer protocol that provides reliable, message-oriented communication between two endpoints. It is commonly used in telecommunications and signaling applications.

IMCP: (Internet Control Message Protocol) is a network-layer protocol that is used for diagnostic and control purposes in IP networks. It is primarily used for communication between network devices and provides feedback, error reporting, and network troubleshooting capabilities. ICMP operates on top of the Internet

Protocol (IP) and is designed to send control messages between network devices.

There were not too many differences in my investigation of the employee PCAP file using NetworkMiner and Wireshark. I felt like Wireshark did give me more insight into how the clients and servers communicated with each other and made it easier to see how different protocols fell into place throughout the time frame captured with the coloring rules setting (extremely helpful).

I would say that Wireshark does have different utilities that make it a more versatile packing sniffing tool than NetworkMiner. If I had to choose one, I would choose Wireshark - this is because it has more tools and applications built into it (although I'm sure I didn't scratch the surface with either tool by any means) and also I think the interface is nicer than NetworkMiner. If I didn't have a choice I would probably use both as they are both great applications to have in one's toolkit.

- And finally, describe the differences between your findings based on **NetworkMiner** and your findings based on **Wireshark**. Are these two tools different in any important ways? Is one more useful than the other in some specific way? Do you prefer one over the other? Or would you want to have both on hand for future PCAP investigations?

NetworkMiner Investigation

Open Questions:

- What is an ‘NIC Vendor’?
- Answer: An "NIC vendor" refers to a company or manufacturer that produces Network Interface Cards (NICs). NICs are hardware devices that enable computers to connect to networks, such as Ethernet or Wi-Fi networks. They provide the physical connection between a computer and the network infrastructure, allowing the computer to send and receive data over the network

- What happens when you receive more packets than you send?
- Answer/Explanation: When you receive more packets than you send, it generally means that you are receiving more data or network traffic than you are actively transmitting. This can occur in various scenarios and can have different implications depending on the context. Here are a few possible scenarios:
Asymmetric Network Traffic: In certain network setups, such as client-server architectures or peer-to-peer networks, it is common to have uneven network traffic patterns. For example, a client may receive more data packets from a server than it sends, especially in scenarios where the server is providing a service or delivering content to the client.

- What are the 'Type' column values in the DNS tab in NetworkMiner? (query)
- Answer/Explanation: In the DNS tab of NetworkMiner, the "Type" column represents the type of DNS resource record (RR) associated with each DNS query or response. DNS resource records provide specific types of information about a domain name within the DNS system. The "Type" column displays the type of resource record for each DNS entry. A: The "A" record maps a domain name to an IPv4 address. It associates a hostname with its corresponding IPv4 address. CNAME: The "CNAME" record defines an alias or canonical name for a domain. It allows a domain name to be an alias for another domain, enabling multiple domain names to resolve to the same IP address.

- What are the ‘Parameter Name’ and ‘Parameter Value’ columns?
- Answer/Explanation: The parameters tab displays all sorts of information extracted from network traffic where there is a notion of a name-and-value combination. NetworkMiner extracts parameters such as HTTP query string names and values, HTTP POST variables, HTTP cookie parameters and FTP commands

- What is the 'Sessions' tab?
- Answer: The "Sessions" tab in the NetworkMiner application displays information about the network sessions captured during packet analysis. A network session refers to a logical connection established between two devices or hosts over a network.

- What is the 'DNS' tab?
- Answer: The "DNS" tab in the NetworkMiner application refers to a section that displays information related to the Domain Name System (DNS) activity captured during network packet analysis.

- Difference between the server host and client host?
- Answer: Server Host: A server host is a device or computer on a network that provides services or resources to other devices, known as clients. Servers are designed to respond to requests from clients and fulfill those requests by providing data, services, or access to shared resources. Examples of server hosts include web servers, file servers, email servers, and database servers. Server hosts typically have static IP addresses and are configured to listen for incoming requests from clients.
Client Host: A client host, on the other hand, is a device or computer that requests and utilizes services or resources from server hosts. Clients initiate communication by sending requests to server hosts and receive responses in return. Clients can be desktop computers, laptops, smartphones, or any other device that accesses services or resources provided by server hosts. Client hosts usually have dynamic IP addresses and are responsible for making requests and handling responses from servers