Executive Summary

In the analysis of the employee's PCAP, no definitive evidence of malicious activity was found. The following is a breakdown of the employee's actions that were captured from the PCAP file: The employee logged on, opened a Mozilla FireFox browser, and navigated to google.com (host interaction: 74.125.225.180). From there, a query for 'fire tornado' was made (host interaction: 74.125.225.101) and several files were downloaded there after (host interaction: 74.125.225.18 & 63.245.215.56). After verification, these files were downloaded from and through credible and secure sources (1 from Google, and 2 through Mozilla hosts). The website 'zeemud.org' was also visited (host interaction 209.128.72.218), and upon further investigation, is a site that hosts a "swords and sorcery themed" text-based role-playing game (most likely where the search for 'fire tornado' stems from). Although the visiting of this site seems to be mostly safe, the act itself does open up the potential for outside malicious activity.

A recommendation (on my behalf) for potential next steps would be to verify if our organization has an Acceptable Use Policy (AUP) in place, whether we formally require employees to review this document, and (if applicable) verify if the employee violated this policy.

This is a solid summary, but let's skip the nitty-gritty details like IP addresses. Those are the kind of things a non-tech manager might not grasp. Remember, your manager may not have a tech background. Here's the type of information that a non-tech manager can easily understand and digest:

```
In this PCAP's short timeframe, the employee we're investigating first
used Google to search for fire tornadoes. They then downloaded some
Firefox browser documentation before visiting the game site zeemud.org.
Currently, we have no evidence of any malicious activities. However, we
should consider if this employee might have violated the corporate
Acceptable Use Policy.
```

Assume your manager is time-crunched, eager to move on, and mainly interested in figuring out what, if anything, needs to be done about this investigation. They don't want to sift through a ton of text—they want you to distill everything down to a concise and reader-friendly format. Your ability to produce short, clear summary statements is just as important as your technical skills. It's relatively easy to find people with strong technical know-how, but it's much harder to find tech-savvy individuals who can communicate effectively.

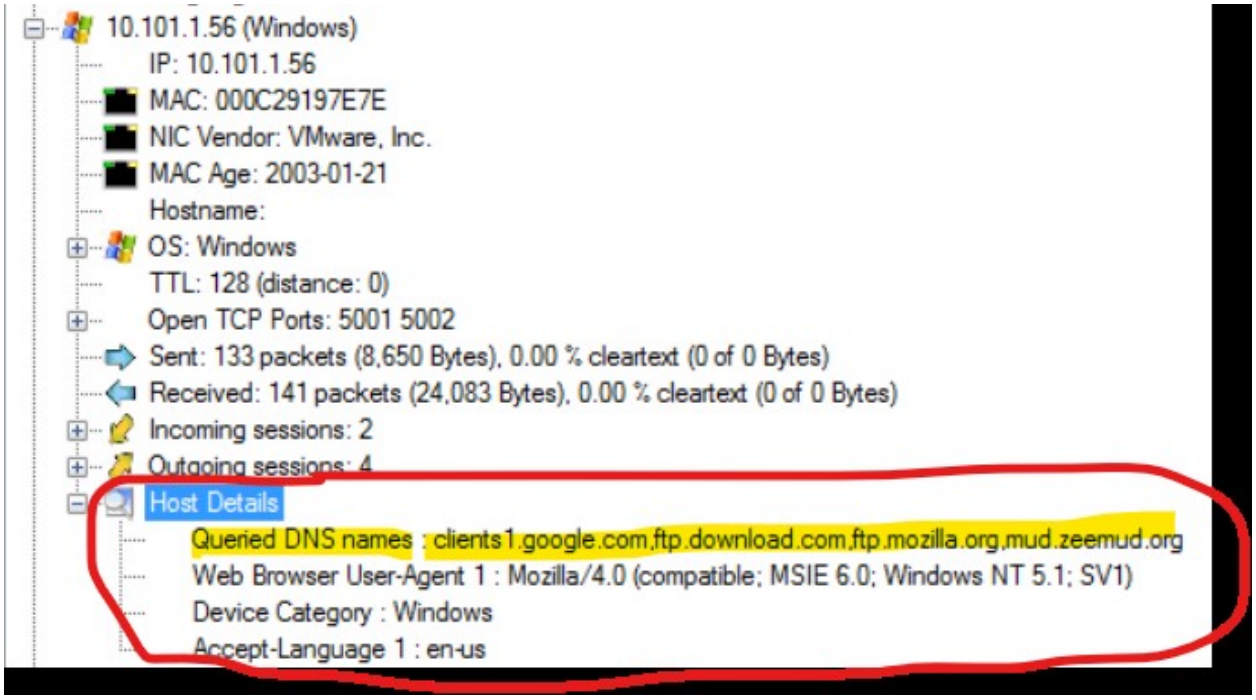
Technical Appendix

Active Hypotheses:

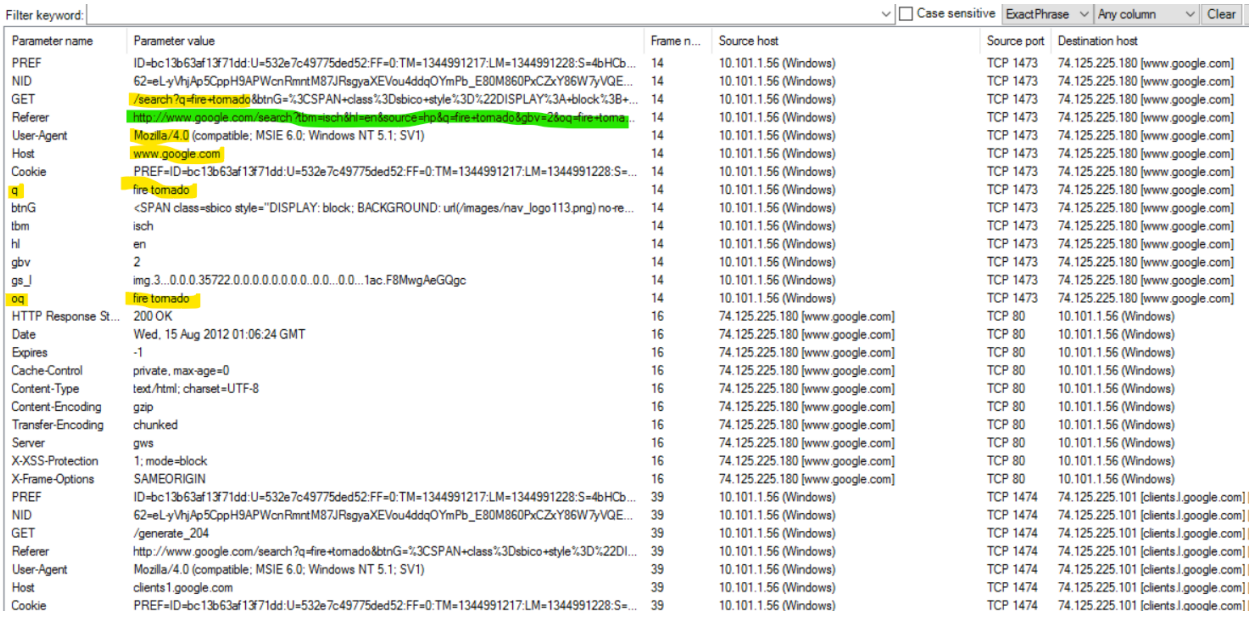
Employee got online, opened up a Mozilla Firefox browser, went to google, searched 'fire tornado', downloaded a few files and visited 'zeemud.org' (what appears to be a game site).

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

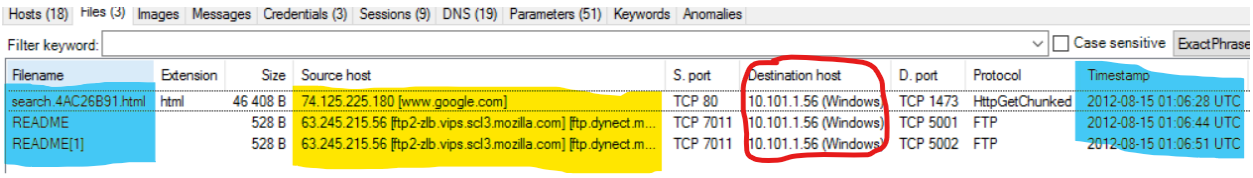
Verified Facts:

- *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.



Self-Directed Learning

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

==========

Reflection Questions

1 What privacy issues arise when you monitor a user's network traffic at work?

If it's in a packet, do you have the right to look at it?

How can you respect employees' privacy while still maintaining sufficient visibility into their activities to protect them from potential threats?

2 When an employee's web traffic is encrypted by SSL, how are you able to distinguish between legitimate and malicious (or risky) network traffic?

What tools do you have available to you in your investigative environments that might allow you to maintain sufficient visibility into encrypted network traffic?

What potential security concerns might decrypting SSL traffic present in an organization?

Is MITMing employee traffic with proxies ethical as long as it is being done by the employer?

3 Should this FTP traffic have been allowed within the corporate network to begin with?

Should this organization's firewall or IDS (Intrusion Detection System) have flagged or blocked this FTP traffic automatically?

4 Reflect on the process of your investigation.

What went well as you conducted your investigation?
What could you have done better?
What advice would you give a new student who is just beginning this task?

5 Do you like this type of work?

Do you enjoy the process of conducting an investigation?
What parts of the investigation were most enjoyable for you to undertake?
Are you interested in doing this as a career?