

Network Forensic Analysis Report

Complete this report as you complete the Network Activity on Day 3 of class.

Time Thieves

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

Ans. **frank-n-ted.com**

Filter: **ip.src==10.6.12.0/24 or ip.addr==10.6.12.0/24**

ip.src == 10.6.12.0/24

No.	Time	Source	Destination	Protocol	Length	Info
62874	690.883903300	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
62875	690.883867200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any source
62876	690.884720000	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any source
62877	690.885586200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
62878	690.886462100	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any source
62879	690.887744100	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX.local, "QM" query
62880	690.889181100	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
62881	690.890365300	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
62882	690.891348100	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any source
62883	690.892878500	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
62884	690.895479900	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
62885	690.896927900	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
62886	690.898612800	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com
62887	690.902843300	10.6.12.157	10.6.12.12	CLDAP	264	searchRequest(1) "<R00T>" baseObject
62888	690.906623400	10.6.12.12	10.6.12.157	CLDAP	236	searchResEntry(1) "<R00T>" searchResDone(1) success [1]
62889	690.907685500	10.6.12.157	10.6.12.12	TCP	66	49668 -> 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
62890	690.908725300	10.6.12.12	10.6.12.157	TCP	66	389 -> 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256
62891	690.909585100	10.6.12.157	10.6.12.12	TCP	54	49668 -> 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0

Magic cookie: DHCP

- Option: (53) DHCP Message Type (ACK)
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (51) IP Address Lease Time
- Option: (54) DHCP Server Identifier (10.6.12.12)
- Option: (1) Subnet Mask (255.255.255.0)
- Option: (81) Client Fully Qualified Domain Name
- Option: (3) Router
- Option: (6) Domain Name Server
 - Length: 4
 - Domain Name Server: 10.6.12.12
- Option: (15) Domain Name
 - Length: 16
 - Domain Name: frank-n-ted.com
- Option: (255) End
- Option End: 255

2. What is the IP address of the Domain Controller (DC) of the AD network?

Ans. **10.6.12.12**

Filter: **ip.src==10.6.12.0/24 or ip.addr==10.6.12.0/24**

ip.src == 10.6.12.0/24

No.	Time	Source	Destination	Protocol	Length	Info
62874	690.883903300	10.6.12.12	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0xba8bd7f0
62875	690.883867200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.251 for any source
62876	690.884720000	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any source
62877	690.885586200	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
62878	690.886462100	10.6.12.157	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any source
62879	690.887744100	10.6.12.157	224.0.0.251	MDNS	80	Standard query 0x0000 ANY DESKTOP-86J4BX
62880	690.889181100	10.6.12.157	224.0.0.251	MDNS	90	Standard query response 0x0000 A 10.6.12.157
62881	690.890365300	10.6.12.157	224.0.0.252	LLMNR	74	Standard query 0x094f ANY DESKTOP-86J4BX
62882	690.891348100	10.6.12.157	224.0.0.22	IGMPv3	62	Membership Report / Join group 224.0.0.251 for any source
62883	690.892878500	10.6.12.157	10.6.12.12	DNS	96	Standard query 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
62884	690.895479900	10.6.12.12	10.6.12.157	DNS	162	Standard query response 0x9c26 SRV _ldap._tcp.dc._msdcs.frank-n-ted.com
62885	690.896927900	10.6.12.157	10.6.12.12	DNS	90	Standard query 0x838c A frank-n-ted-dc.frank-n-ted.com
62886	690.898612800	10.6.12.12	10.6.12.157	DNS	106	Standard query response 0x838c A frank-n-ted-dc.frank-n-ted.com
62887	690.902843300	10.6.12.157	10.6.12.12	CLDAP	264	searchRequest(1) "<R00T>" baseObject
62888	690.906623400	10.6.12.12	10.6.12.157	CLDAP	236	searchResEntry(1) "<R00T>" searchResDone(1) success [1]
62889	690.907685500	10.6.12.157	10.6.12.12	TCP	66	49668 -> 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
62890	690.908725300	10.6.12.12	10.6.12.157	TCP	66	389 -> 49668 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256
62891	690.909585100	10.6.12.157	10.6.12.12	TCP	54	49668 -> 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0

Magic cookie: DHCP

- Option: (53) DHCP Message Type (ACK)
- Option: (58) Renewal Time Value
- Option: (59) Rebinding Time Value
- Option: (51) IP Address Lease Time
- Option: (54) DHCP Server Identifier (10.6.12.12)
- Option: (1) Subnet Mask (255.255.255.0)
- Option: (81) Client Fully Qualified Domain Name
- Option: (3) Router
- Option: (6) Domain Name Server
 - Length: 4
 - Domain Name Server: 10.6.12.12
- Option: (15) Domain Name
 - Length: 16
 - Domain Name: frank-n-ted.com
- Option: (255) End
- Option End: 255

Ans. **june11.dll**

Filter: **ip.addr==10.6.12.203 and http.request.method==GET**

The image shows a Wireshark packet capture with a filter of `ip.addr==10.6.12.203 and http.request.method==GET`. The packet list shows two packets: packet 66512 (GET /pQBtWj HTTP/1.1) and packet 66516 (GET /files/june11.dll HTTP/1.1). Packet 66516 is selected, and the packet details pane shows the following information:

- Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104
- Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
- Hypertext Transfer Protocol
 - GET /files/june11.dll HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /files/june11.dll
 - Request Version: HTTP/1.1
 - Accept: */*\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
 - Host: 205.185.125.104\r\n
 - Connection: Keep-Alive\r\n
 - Cookie: _subid=3mmhfnd8jp\r\n
 - \r\n
 - [Full request URI: http://205.185.125.104/files/june11.dll]

4. Upload the file to [VirusTotal.com] (<https://www.virustotal.com/gui/>).

Ans. **Googleipdate**

The image shows a Wireshark packet capture with a filter of `ip.addr==10.6.12.203 and http.request.method==GET`. The packet list shows two packets: packet 66512 (GET /pQBtWj HTTP/1.1) and packet 66516 (GET /files/june11.dll HTTP/1.1). Packet 66516 is selected, and the packet details pane shows the following information:

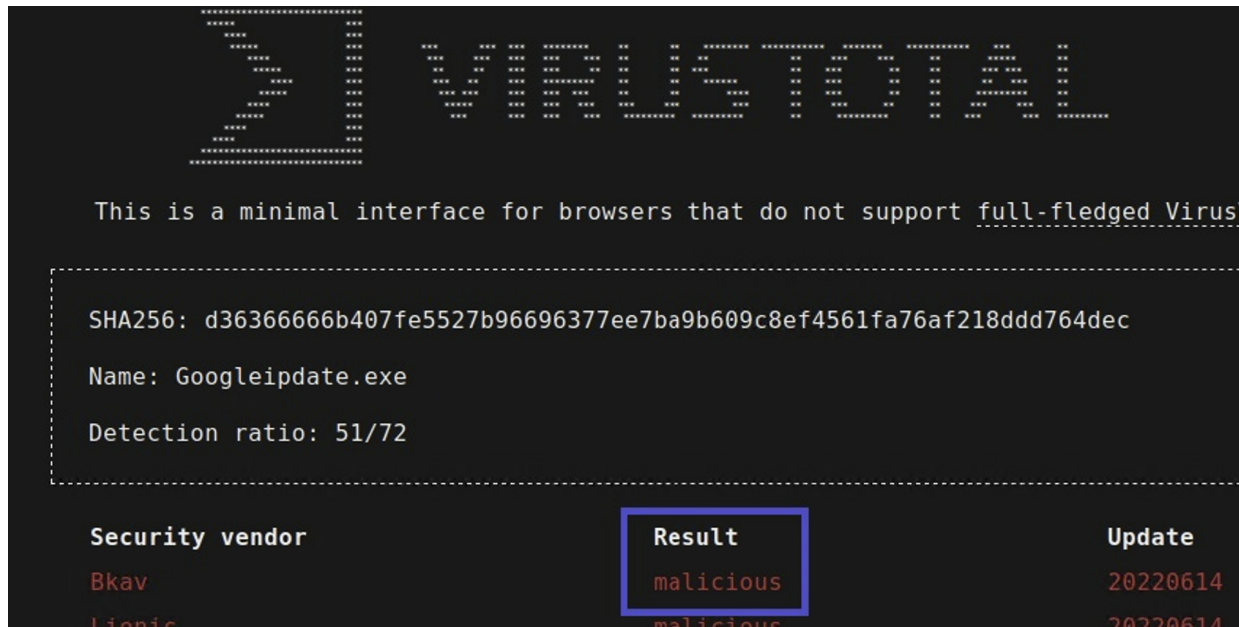
- Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104
- Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
- Hypertext Transfer Protocol
 - GET /files/june11.dll HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /files/june11.dll HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /files/june11.dll
 - Request Version: HTTP/1.1
 - Accept: */*\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
 - Host: 205.185.125.104\r\n
 - Connection: Keep-Alive\r\n
 - Cookie: _subid=3mmhfnd8jp\r\n
 - \r\n
 - [Full request URI: http://205.185.125.104/files/june11.dll]

What kind of malware is this classified as?

The image shows the VirusTotal scan results for a file named **Googleipdate.exe**. The SHA256 hash is `d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec`. The detection ratio is 51/72. The results are as follows:

Security vendor	Result	Update
Bkav	malicious	20220614
Lionic	malicious	20220614

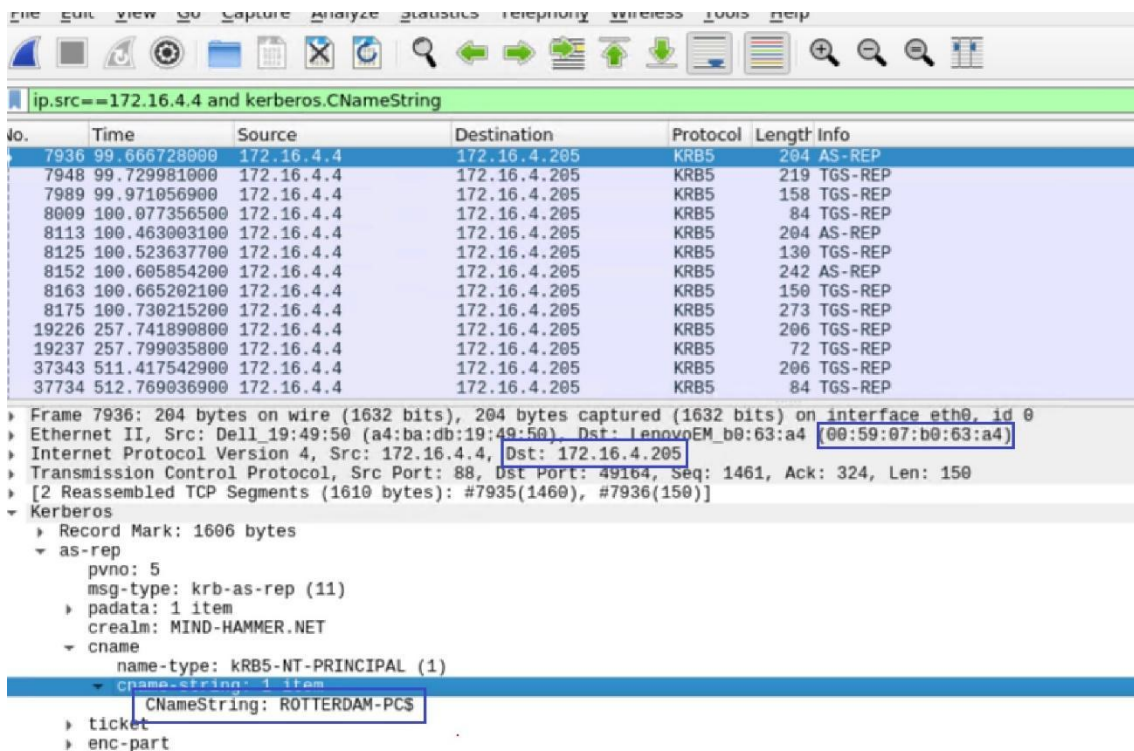
Ans. **Malicious**



Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:

- Host name: **ROTTERDAM-PC\$**
- IP address: **172.16.4.205**
- MAC address: **00:59:07:b0:63:a4**



2. What is the username of the Windows user whose computer is infected?

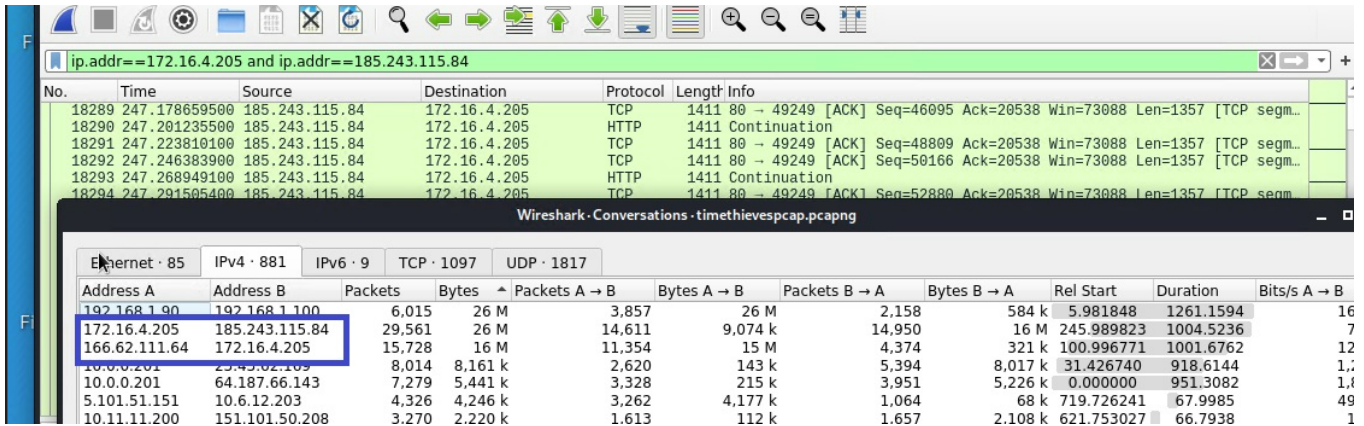
Ans:

Filter: **ip.src==172.16.4.205 and Kerberos.CNameString**

3. What are the IP addresses used in the actual infection traffic?

Ans. IP addresses used in the actual infection traffic are:

166.62.111.64
172.16.4.205
185.243.115.84



No.	Time	Source	Destination	Protocol	Length	Info
18289	247.178659500	185.243.115.84	172.16.4.205	TCP	1411	80 → 49249 [ACK] Seq=46095 Ack=20538 Win=73088 Len=1357 [TCP segm...]
18290	247.201235500	185.243.115.84	172.16.4.205	HTTP	1411	Continuation
18291	247.223810100	185.243.115.84	172.16.4.205	TCP	1411	80 → 49249 [ACK] Seq=48809 Ack=20538 Win=73088 Len=1357 [TCP segm...]
18292	247.246383900	185.243.115.84	172.16.4.205	TCP	1411	80 → 49249 [ACK] Seq=50166 Ack=20538 Win=73088 Len=1357 [TCP segm...]
18293	247.268949100	185.243.115.84	172.16.4.205	HTTP	1411	Continuation
18294	247.291505400	185.243.115.84	172.16.4.205	TCP	1411	80 → 49249 [ACK] Seq=52880 Ack=20538 Win=73088 Len=1357 [TCP segm...]

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B
192.168.1.90	192.168.1.100	6,015	26 M	3,857	26 M	2,158	584 k	5.981848	1261.1594	16
172.16.4.205	185.243.115.84	29,561	26 M	14,611	9,074 k	14,950	16 M	245.989823	1004.5236	7
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	100.996771	1001.6762	12
10.0.0.201	25.45.82.109	8,014	8,161 k	2,620	143 k	5,394	8,017 k	31.426740	918.6144	1,7
10.0.0.201	64.187.66.143	7,279	5,441 k	3,328	215 k	3,951	5,226 k	0.000000	951.3082	1,7
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	719.726241	67.9985	49
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	621.753027	66.7938	1

4. As a bonus, retrieve the desktop background of the Windows host.

Ans. **Two Windows desktop background were retrieved by exporting objects: File > Export Objects > HTTP**

