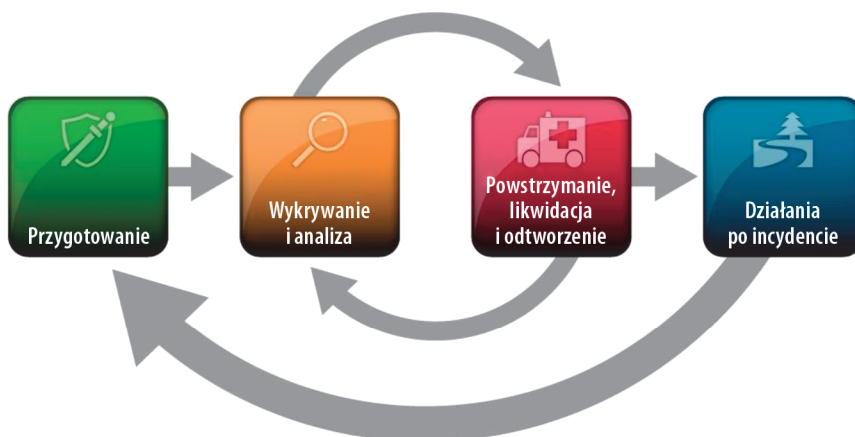


ROZDZIAŁ 1.

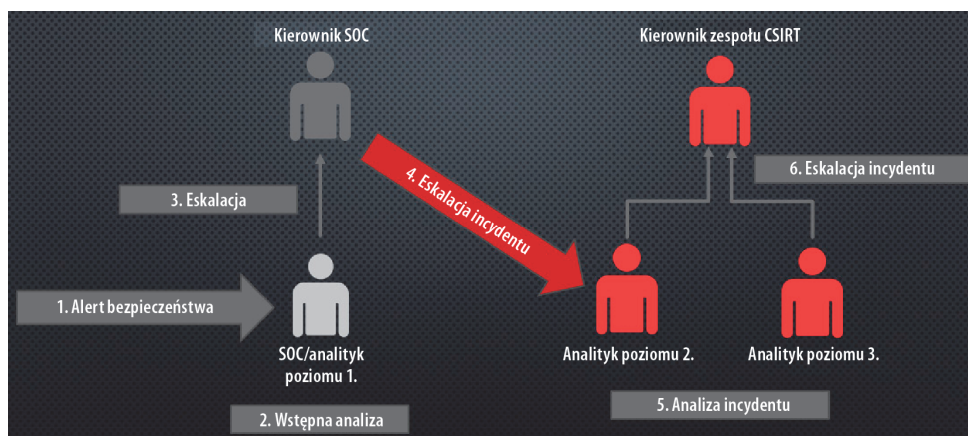
Czym jest reagowanie na incydenty



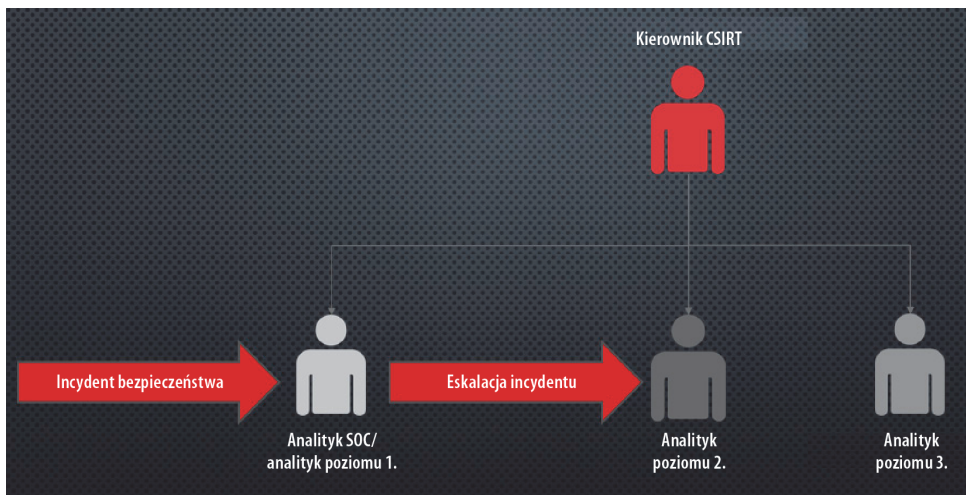
Rysunek 1.1. Proces reagowania na incydenty NIST

ROZDZIAŁ 2.

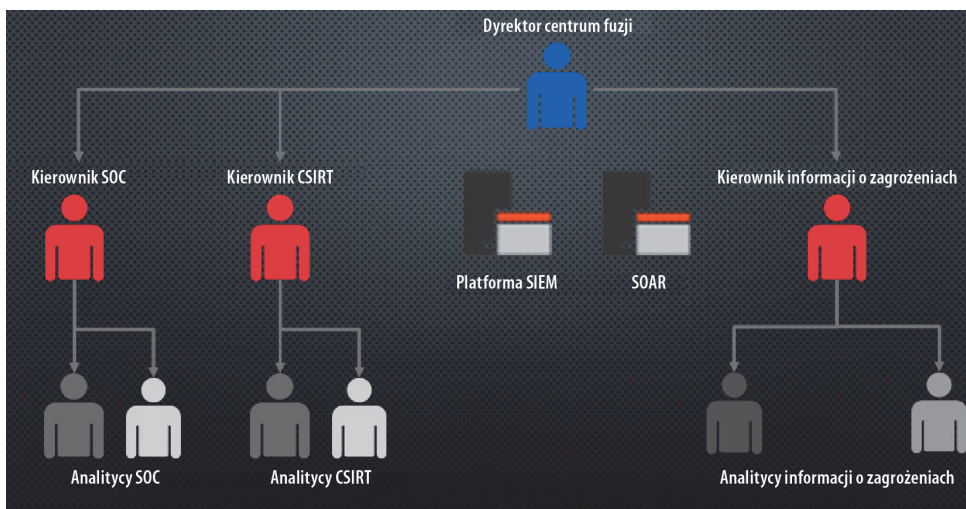
Zarządzanie incydentami cyberbezpieczeństwa



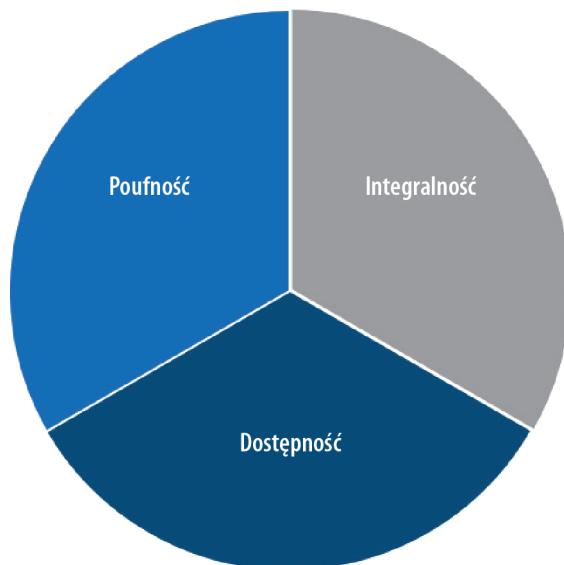
Rysunek 2.1. Model angażowania SOC



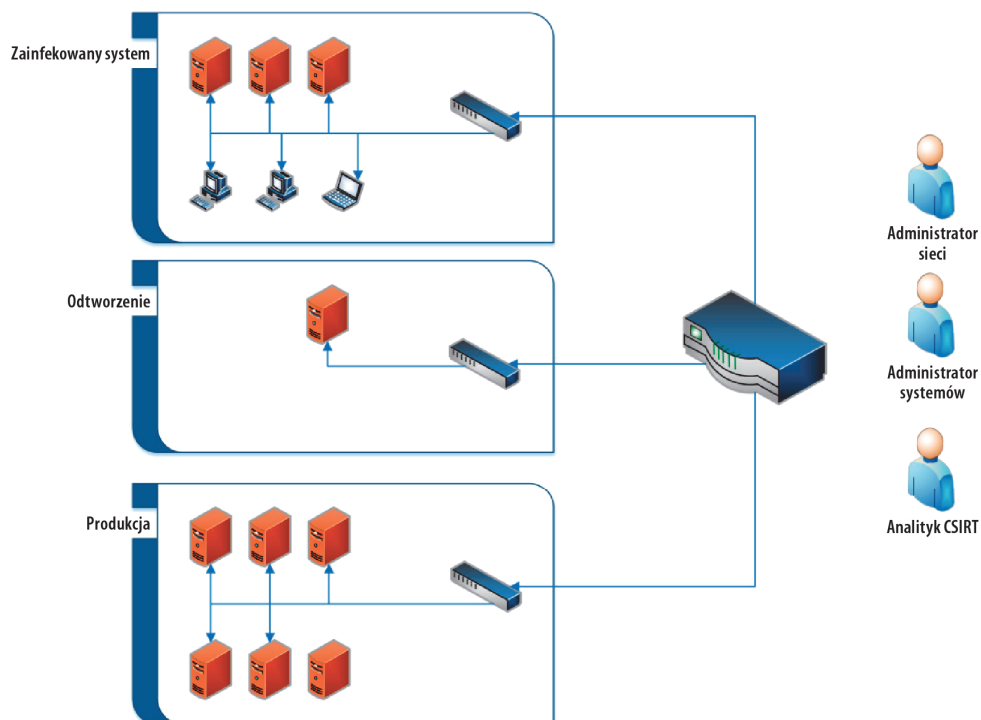
Rysunek 2.2. Zintegrowany model SOC



Rysunek 2.3. Model centrum fuzji



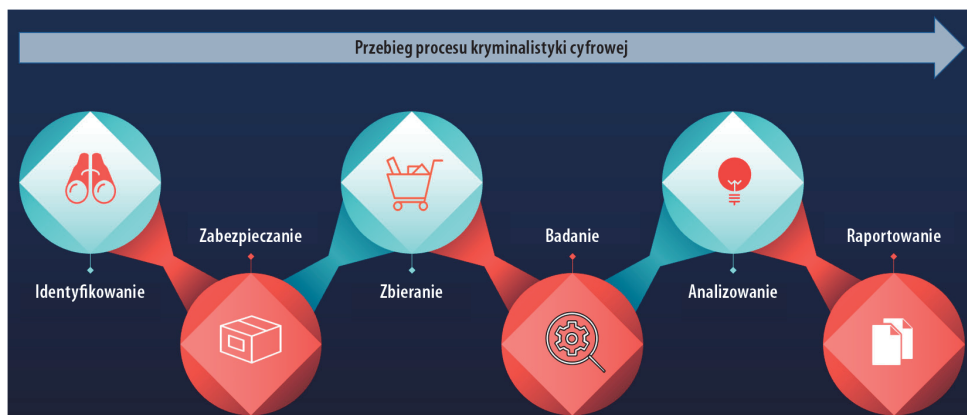
Rysunek 2.4. Triada CIA



Rysunek 2.5. Usunięcie systemu i architektura jego odtwarzania

ROZDZIAŁ 3.

Podstawy kryminalistyki cyfrowej



Rysunek 3.1. Przebieg procesu kryminalistyki cyfrowej



Rysunek 3.7. Fizyczna blokada zapisu



Rysunek 3.8. System operacyjny DEFT przeznaczony na potrzeby kryminalistyki cyfrowej



Rysunek 3.9. System operacyjny CAINE przeznaczony na potrzeby kryminalistyki cyfrowej



Rysunek 3.10. Stacja robocza SANS SIFT



Rysunek 3.11. System operacyjny CSI Linux przeznaczony na potrzeby kryminalistyki cyfrowej



Rysunek 3.12. System operacyjny REMNIX przeznaczony na potrzeby kryminalistyki cyfrowej

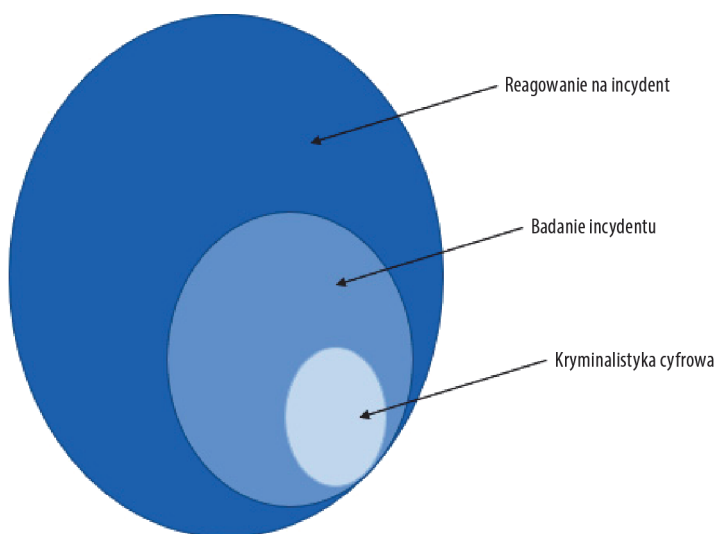


Rysunek 3.13. Zestaw przenośny do zastosowań w kryminalistyce cyfrowej

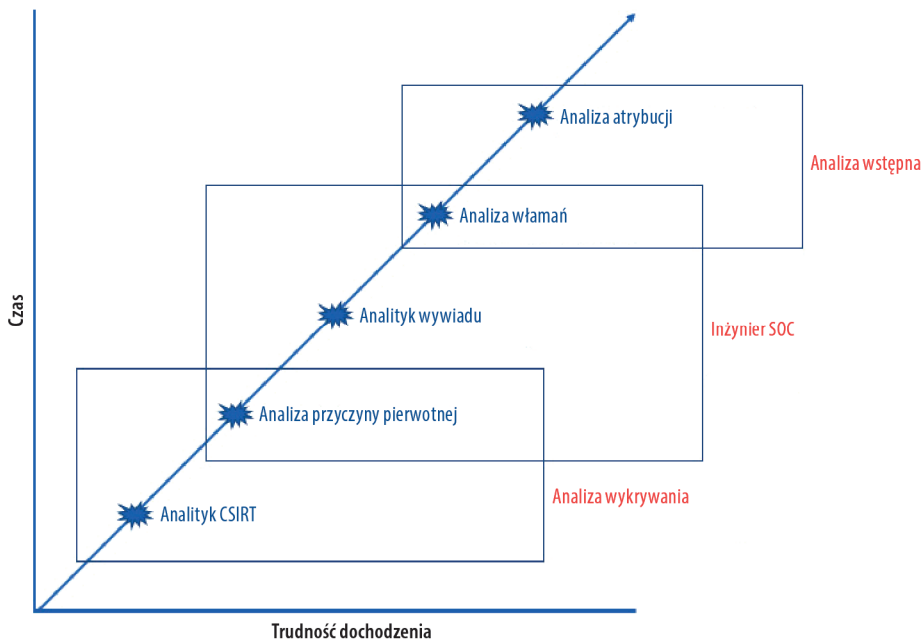


Rysunek 3.14. Zawartość zestawu przenośnego

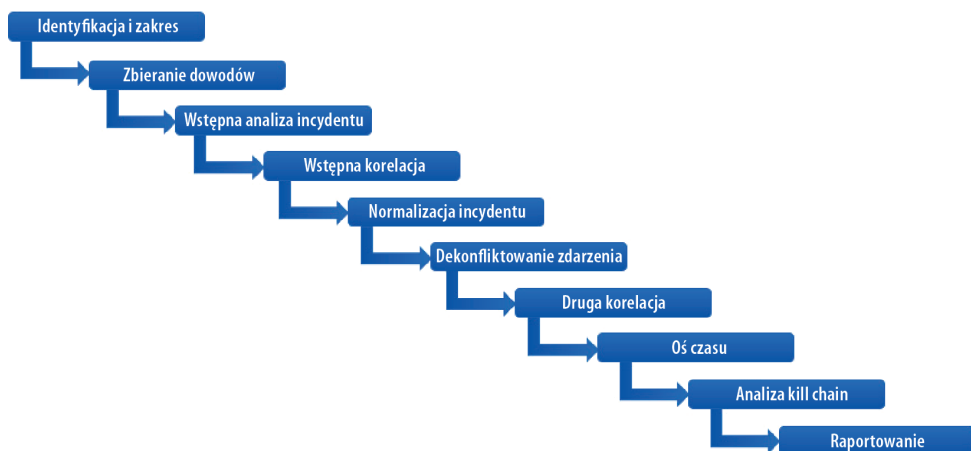
ROZDZIAŁ 4. Metoda dochodzeniowa



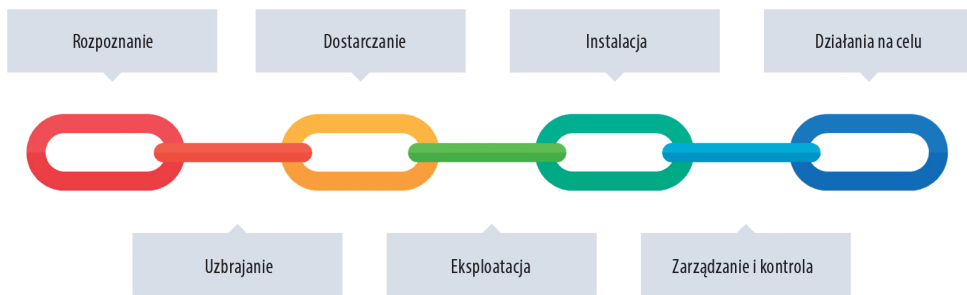
Rysunek 4.1. Związek między kryminalistyką cyfrową, badaniem incydentów a reagowaniem na incydenty



Rysunek 4.2. Rodzaje dochodzeń prowadzonych w sprawie incydentów cyfrowych

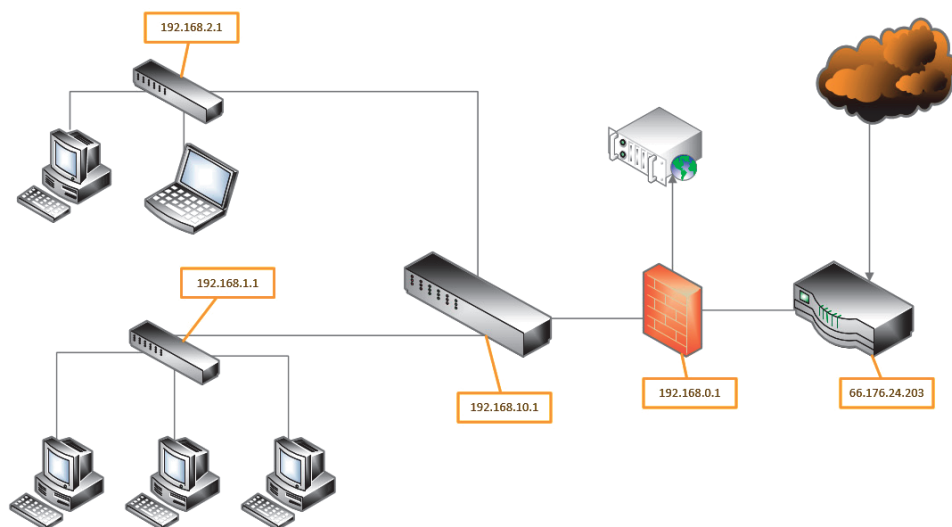


Rysunek 4.3. Dziesięcioetapowa metodyka dochodzenia

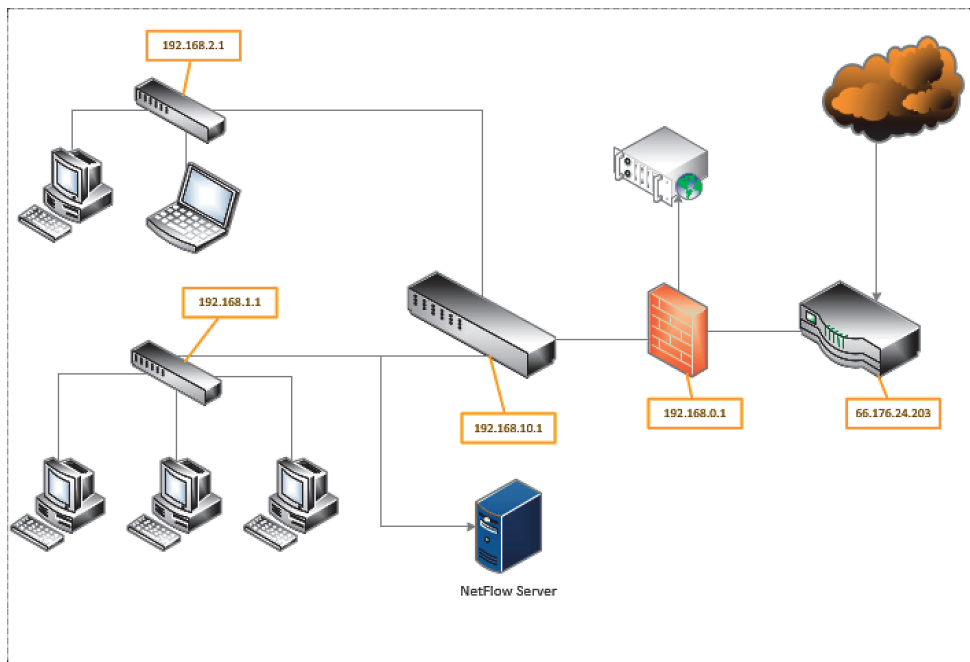


Rysunek 4.4. Łańcuch kill chain

ROZDZIAŁ 5. Zbieranie dowodów sieciowych



Rysunek 5.1. Przykładowy schemat sieci



Rysunek 5.2. Diagram NetFlow

ping_capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.49.136	8.8.8.8	ICMP	98	Echo (ping) request
2	0.020701	8.8.8.8	192.168.49.136	ICMP	98	Echo (ping) reply
3	1.001149	192.168.49.136	8.8.8.8	ICMP	98	Echo (ping) request
4	1.148688	8.8.8.8	192.168.49.136	ICMP	98	Echo (ping) reply
5	2.001195	192.168.49.136	8.8.8.8	ICMP	98	Echo (ping) request
6	2.021638	8.8.8.8	192.168.49.136	ICMP	98	Echo (ping) reply
7	3.002919	192.168.49.136	8.8.8.8	ICMP	98	Echo (ping) request
8	3.028110	8.8.8.8	192.168.49.136	ICMP	98	Echo (ping) reply
9	3.234573	Vmware_1f:03:2e	Vmware_c2:60:2f	ARP	42	Who has 192.168.49.2?
10	3.234851	Vmware_e2:60:2f	Vmware_1f:03:2e	ARP	60	192.168.49.2 is at 00

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)

Ethernet II, Src: Vmware_1f:03:2e (00:0c:29:1f:03:2e), Dst: Vmware_e2:60:2f (00:50:56:e2:60:2f)

Internet Protocol Version 4, Src: 192.168.49.136, Dst: 8.8.8.8

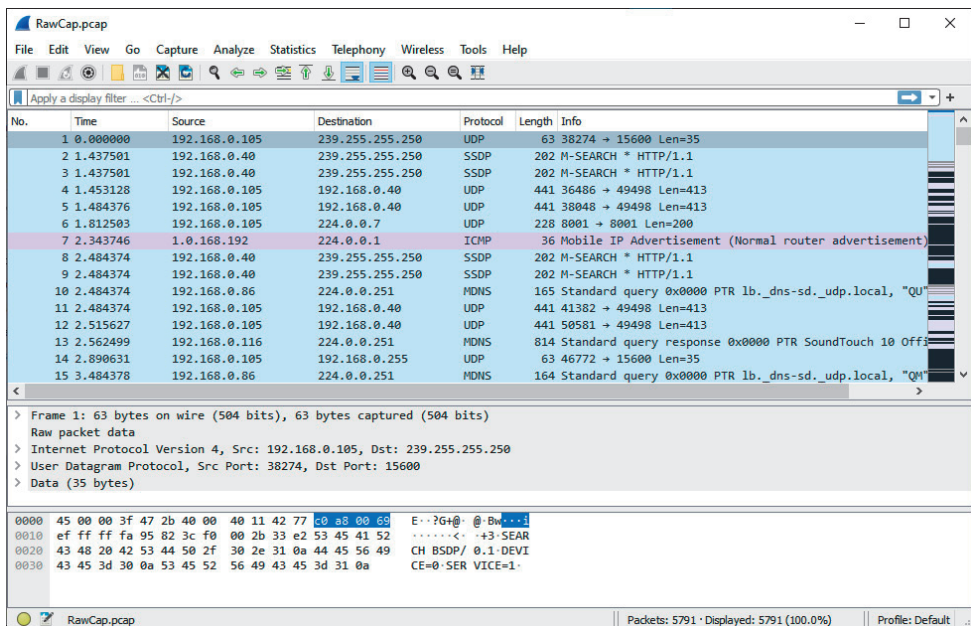
Internet Control Message Protocol

```

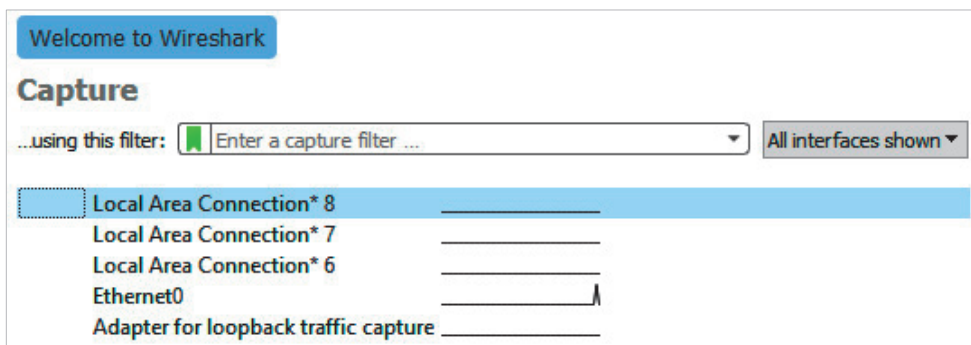
0000  00 50 56 e2 60 2f 00 0c 29 1f 03 2e 08 00 45 00  -PV../..}...E-
0010  00 54 e4 50 40 00 40 01 54 18 c0 a8 31 88 08 08  -T.P@.T...1...
0020  08 08 08 00 bb 6a 9c 5e 00 04 83 84 17 5d 00 00  -...j.A.....]...
0030  00 00 38 7e 0e 00 00 00 00 00 10 11 12 13 14 15  -..8....."#$%
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  -.....!""#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  -&'()*+,-./012345
0060  36 37  -67
  
```

ping_capture Packets: 8049 · Displayed: 8049 (100.0%) Profile: Default

Rysunek 5.7. Analiza przechwytywanych pakietów w programie Wireshark



Rysunek 5.10. Analiza pliku RawCap w programie Wireshark



Rysunek 5.11. Interfejsy przechwytywania programu Wireshark

Capturing from Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
17228	35.386167	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=1993713 Ack=17240 Win=64128 Len=14
17229	35.386179	192.168.0.40	104.71.218.153	TCP	54	25963 → 443 [ACK] Seq=17240 Ack=1995173 Win=525568 Len=0
17230	35.386223	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=1995173 Ack=17240 Win=64128 Len=14
17231	35.386223	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=1996633 Ack=17240 Win=64128 Len=14
17232	35.386223	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=1998093 Ack=17240 Win=64128 Len=14
17233	35.386223	104.71.218.153	192.168.0.40	TLSv1.3	400	Application Data
17234	35.386238	192.168.0.40	104.71.218.153	TCP	54	25963 → 443 [ACK] Seq=17240 Ack=1999899 Win=525568 Len=0
17235	35.386918	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=1999899 Ack=17240 Win=64128 Len=14
17236	35.386965	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=2001359 Ack=17240 Win=64128 Len=14
17237	35.386965	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=2002819 Ack=17240 Win=64128 Len=14
17238	35.386965	104.71.218.153	192.168.0.40	TCP	1514	443 → 25963 [ACK] Seq=2004279 Ack=17240 Win=64128 Len=14
17239	35.386978	192.168.0.40	104.71.218.153	TCP	54	25963 → 443 [ACK] Seq=17240 Ack=2005739 Win=525568 Len=0
17240	35.387203	104.71.218.153	192.168.0.40	TLSv1.3	607	Application Data
17241	35.494596	192.168.0.40	104.71.218.153	TCP	54	25963 → 443 [ACK] Seq=17240 Ack=2006292 Win=524800 Len=0

< >

> Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{3FA55868-6259-47EE-955A-AACC518CAF07}, interface 0

> Ethernet II, Src: 8a:cc:9c:e4:88:44 (8a:cc:9c:e4:88:44), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 52038, Dst Port: 15600

> Data (35 bytes)

< >

```

0000  01 00 5e 7f ff fa 8a cc 9c e4 88 44 08 00 45 00  ..^.....D..E..
0010  00 3f 38 af 40 00 40 11 50 f3 c0 a8 00 69 ff ff  ..8.@.P....i..
0020  ff fa cb 46 3c f0 00 2b fe 1d 53 45 41 52 43 48  ..F<...SEARCH
0030  20 42 53 44 50 2f 30 2e 31 0a 44 45 56 49 43 45  BSDP/0.1.DEVICE
0040  3d 30 0a 53 45 52 56 49 43 45 3d 31 0a          =0.SERVICEL

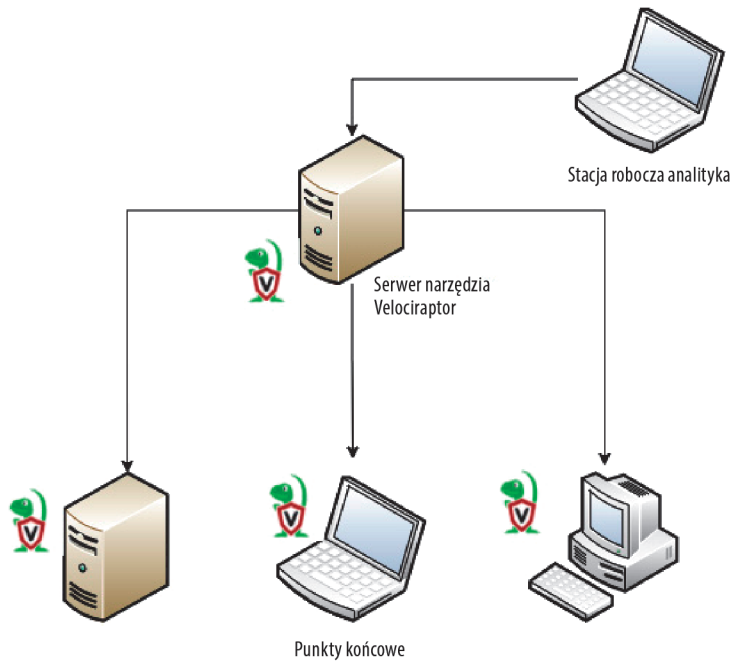
```

Ethernet0: <live capture in progress> | Packets: 17241 | Displayed: 17241 (100.0%) | Profile: Default

Rysunek 5.12. Widok przechwytywania programu Wireshark

ROZDZIAŁ 7.

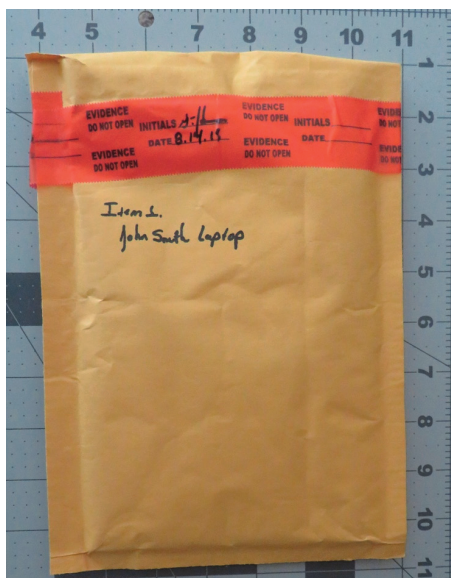
Zdalne gromadzenie dowodów



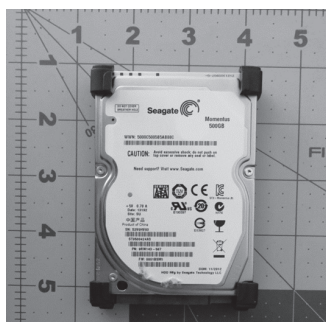
Rysunek 7.1. Konfiguracja narzędzia Velociraptor

ROZDZIAŁ 8.

Obrazowanie kryminalistyczne



Rysunek 8.8. Kontrola integralności opakowania

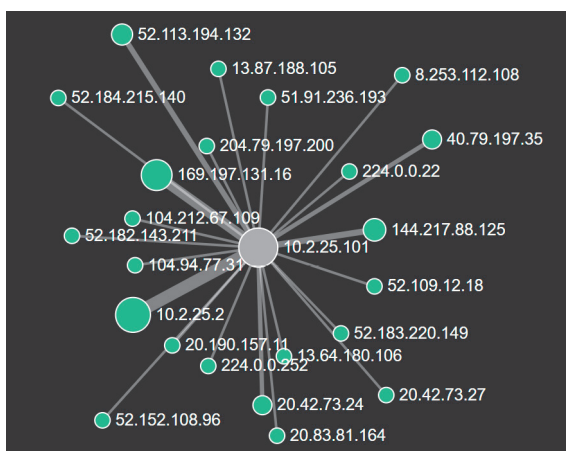


Rysunek 8.9. Przykładowe zdjęcie dysku



Rysunek 8.10. Konfiguracja fizycznej blokady zapisu

ROZDZIAŁ 9. Badanie dowodów sieciowych



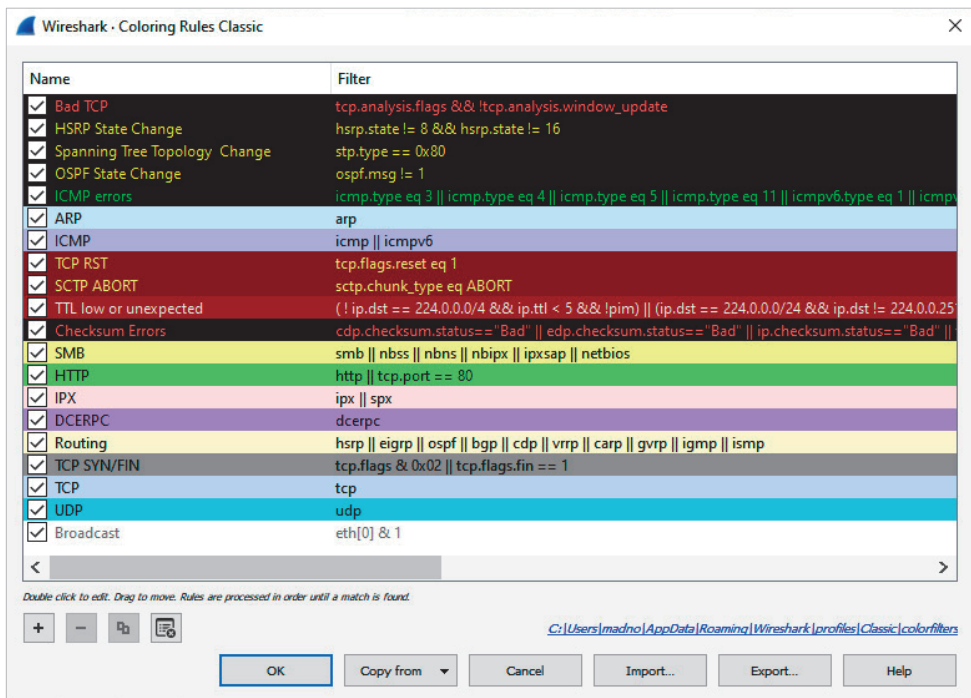
Rysunek 9.18. Wykres połączeń w Arkime

No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	10.4.14.101	TCP
731	85.565098	10.4.14.101	204.79.197.219	TCP
732	85.565175	204.79.197.219	10.4.14.101	TCP
733	85.565175	10.4.14.101	204.79.197.219	TCP
734	85.565348	204.79.197.219	10.4.14.101	TCP
735	85.565380	204.79.197.219	10.4.14.101	TLSv1.2
736	85.565380	10.4.14.101	204.79.197.219	TCP
737	85.611504	10.4.14.101	10.4.14.4	DNS
738	85.613032	10.4.14.101	204.79.197.219	TCP
739	85.895409	10.4.14.101	10.4.14.4	DNS
740	85.945248	10.4.14.4	10.4.14.101	DNS
741	85.946784	10.4.14.101	208.91.198.131	TCP
742	86.108025	208.91.198.131	10.4.14.101	TCP
743	86.108518	10.4.14.101	208.91.198.131	TCP
744	86.109239	10.4.14.101	208.91.198.131	HTTP
745	86.200705	10.4.14.101	239.255.255.250	SSDP
746	86.235023	10.4.14.101	224.0.0.251	MDNS
747	86.236306	208.91.198.131	10.4.14.101	TCP
748	87.170753	208.91.198.131	10.4.14.101	HTTP
749	87.214232	10.4.14.101	208.91.198.131	TCP
750	87.227980	10.4.14.101	208.91.198.131	HTTP
751	87.443277	208.91.198.131	10.4.14.101	TCP

Rysunek 9.19. Widok adresów IP w narzędziu Wireshark

No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	DESKTOP-S9U1NBH.loc...	TCP
731	85.565098	DESKTOP-S9U1NBH.1...	204.79.197.219	TCP
732	85.565175	204.79.197.219	DESKTOP-S9U1NBH.loc...	TCP
733	85.565175	DESKTOP-S9U1NBH.1...	204.79.197.219	TCP
734	85.565348	204.79.197.219	DESKTOP-S9U1NBH.loc...	TCP
735	85.565380	204.79.197.219	DESKTOP-S9U1NBH.loc...	TLSv1.2
736	85.565380	DESKTOP-S9U1NBH.1...	204.79.197.219	TCP
737	85.611504	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
738	85.613032	DESKTOP-S9U1NBH.1...	204.79.197.219	TCP
739	85.895409	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
740	85.945248	fbodyguards-dc.fam...	DESKTOP-S9U1NBH.loc...	DNS
741	85.946784	DESKTOP-S9U1NBH.1...	geobram.com	TCP
742	86.108025	geobram.com	DESKTOP-S9U1NBH.loc...	TCP
743	86.108518	DESKTOP-S9U1NBH.1...	geobram.com	TCP
744	86.109239	DESKTOP-S9U1NBH.1...	geobram.com	HTTP
745	86.200705	DESKTOP-S9U1NBH.1...	239.255.255.250	SSDP
746	86.235023	DESKTOP-S9U1NBH.1...	224.0.0.251	MDNS
747	86.236306	geobram.com	DESKTOP-S9U1NBH.loc...	TCP
748	87.170753	geobram.com	DESKTOP-S9U1NBH.loc...	HTTP
749	87.214232	DESKTOP-S9U1NBH.1...	geobram.com	TCP
750	87.227980	DESKTOP-S9U1NBH.1...	geobram.com	HTTP
751	87.443277	geobram.com	DESKTOP-S9U1NBH.loc...	TCP

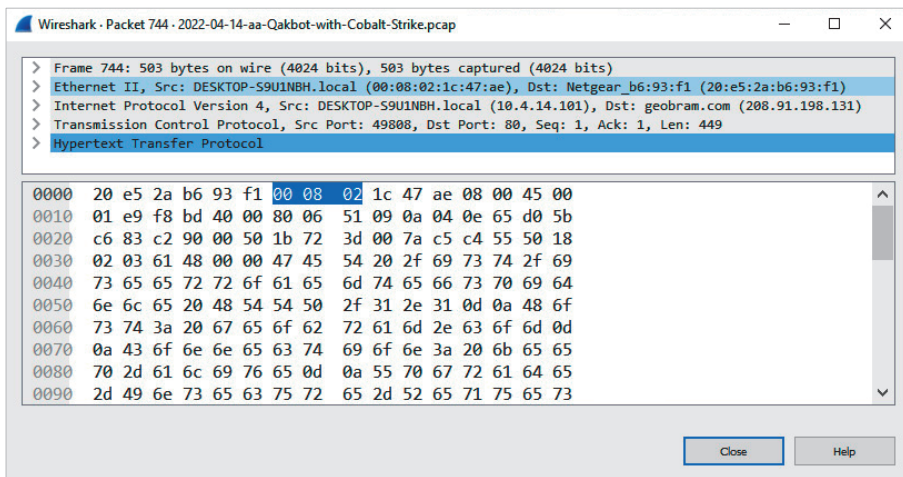
Rysunek 9.20. Widok nazwy domeny w Wiresharku



Rysunek 9.21. Klasyczne zasady kolorowania w Wiresharku

ip.src==10.4.14.101				
No.	Time	Source	Destination	Protocol
7	0.016790	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
8	0.016790	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
11	0.016956	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
12	0.017069	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
13	0.017167	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
15	0.017638	DESKTOP-S9U1NBH.1...	224.0.0.251	MDNS
17	0.017759	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
18	0.017928	DESKTOP-S9U1NBH.1...	224.0.0.252	LLMNR
20	0.019548	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
21	0.019671	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
23	0.020796	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
25	0.024289	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
27	0.025112	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	CLDAP
29	0.077855	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
30	0.078012	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
31	0.078012	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
32	0.139412	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	CLDAP
35	0.249760	DESKTOP-S9U1NBH.1...	igmp.mcast.net	IGMPv3
38	0.252767	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	NTP
40	0.296701	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
42	0.437900	DESKTOP-S9U1NBH.1...	224.0.0.252	LLMNR
43	0.534357	DESKTOP-S9U1NBH.1...	fbodyguards-dc.fant...	DNS
45	0.840349	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS
46	0.840349	DESKTOP-S9U1NBH.1...	10.4.14.255	NBNS

Rysunek 9.22. Filtrowanie po adresach źródłowych



Rysunek 9.23. Dane dotyczące pakietów

No.	Time	Source	Destination	Protocol	Length	Info
744	88.168239	DESKTOP-S9U1NBH.local	geobram.com	HTTP	503	GET /ist/iseerosestefspidnie HTTP/1.1
748	87.178753	geobram.com	DESKTOP-S9U1NBH.local	HTTP	655	HTTP/1.1 200 OK (text/html)
750	87.227880	DESKTOP-S9U1NBH.local	geobram.com	HTTP	606	GET /ist/NO_2950435796.zip HTTP/1.1
1290	92.544164	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	[TCP Previous segment not captured] Continuation
1292	92.544287	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1294	92.544414	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1296	92.544589	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1298	92.544662	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1299	92.544780	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1302	92.544911	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1305	92.546865	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1306	92.547834	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1307	92.547151	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1309	92.550222	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1310	92.550293	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1311	92.550457	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1312	92.550528	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1313	92.550695	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1315	92.550767	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1317	92.550892	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1319	92.551818	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1322	92.553795	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1323	92.553867	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1324	92.554031	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation

Rysunek 9.24. Widok pakietu HTTP

2022-04-14-aa-Qakbot-with-Cobalt-Strike.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

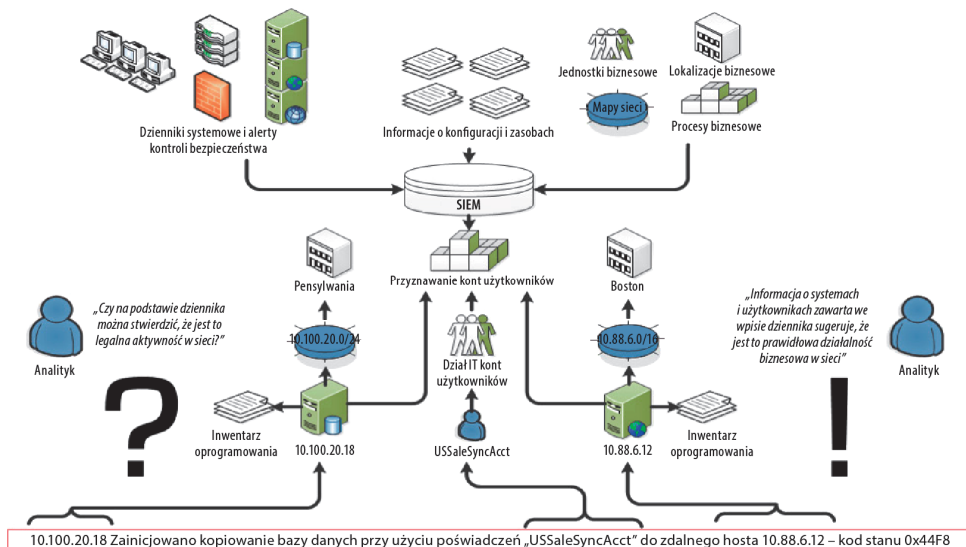
http

No.	Time	Source	Destination	Protocol	Length	Info
744	86.109239	DESKTOP-S9U1NBH.local	geobram.com	HTTP	503	GET /ist/iseerroaentefspidnle HTTP/1.1
748	87.170753	geobram.com	DESKTOP-S9U1NBH.local	HTTP	653	HTTP/1.1 200 OK (text/html)
750	87.227980	DESKTOP-S9U1NBH.local	geobram.com	HTTP	606	GET /ist/NO_2950435796.zip HTTP/1.1
1290	92.544164	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	[TCP Previous segment not captured] Continuation
1292	92.544287	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1294	92.544414	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1296	92.544589	geobram.com	DESKTOP-S9U1NBH.local	HTTP	1442	Continuation
1298	92.544662	geobram.com	Mark/Unmark Packet	Ctrl+M	1442	Continuation
1299	92.544780	geobram.com	Ignore/Unignore Packet	Ctrl+D	1442	Continuation
1302	92.544911	geobram.com	Set/Unset Time Reference	Ctrl+T	1442	Continuation
1305	92.546965	geobram.com	Time Shift...	Ctrl+Shift+T	1442	Continuation
1306	92.547034	geobram.com	Packet Comment...	Ctrl+Alt+C	1442	Continuation
1307	92.547151	geobram.com			1442	Continuation
1309	92.550222	geobram.com			1442	Continuation
1310	92.550293	geobram.com			1442	Continuation
1311	92.550457	geobram.com	Edit Resolved Name		1442	Continuation
1312	92.550528	geobram.com			1442	Continuation
1313	92.550695	geobram.com	Apply as Filter		1442	Continuation
1315	92.550767	geobram.com	Prepare as Filter		1442	Continuation
1317	92.550892	geobram.com	Conversation Filter		1442	Continuation
1319	92.551018	geobram.com			1442	Continuation
1322	92.553795	geobram.com	Colorize Conversation		1442	Continuation
1323	92.553867	geobram.com	SCPT		1442	Continuation
1324	92.554031	geobram.com	Follow		1442	Continuation
Transmission Control Protocol					8874, Ack: 1002, Len: 1388	
Hypertext Transfer Protocol						
File Data: 1388 bytes						
0000 00 08 02 1c 47 ae						
0010 05 94 9a a8 40 00						
0020 0e 65 00 50 c2 90						
Protocol Preferences						
Decode As...						
Show Packet in New Window						

Rysunek 9.25. Śledzenie strumieni HTTP

ROZDZIAŁ 12.

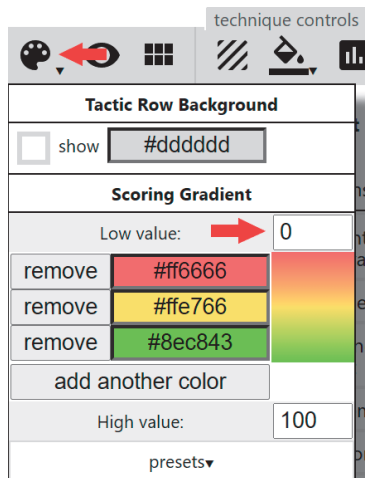
Analizowanie plików dziennika



Rysunek 12.1. SIEM i architektura rejestrowania

ROZDZIAŁ 17.

Korzystanie z analizy cyberzagrożeń



Rysunek 17.14. Wybór koloru tła w narzędziu nawigator w bazie MITRE ATT&CK