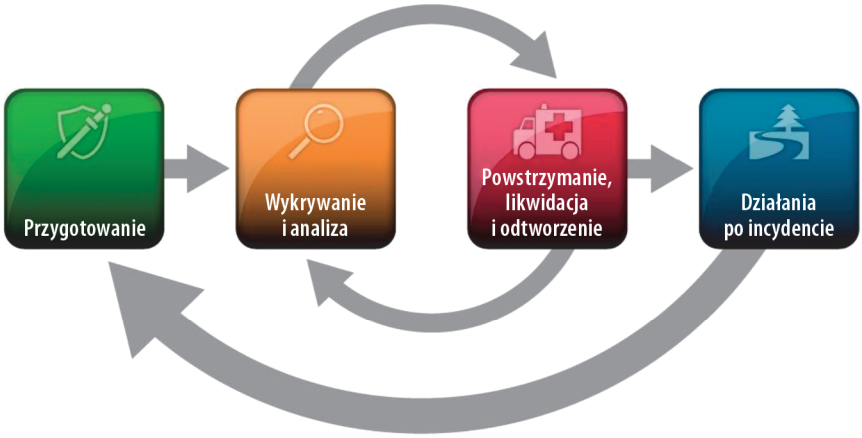
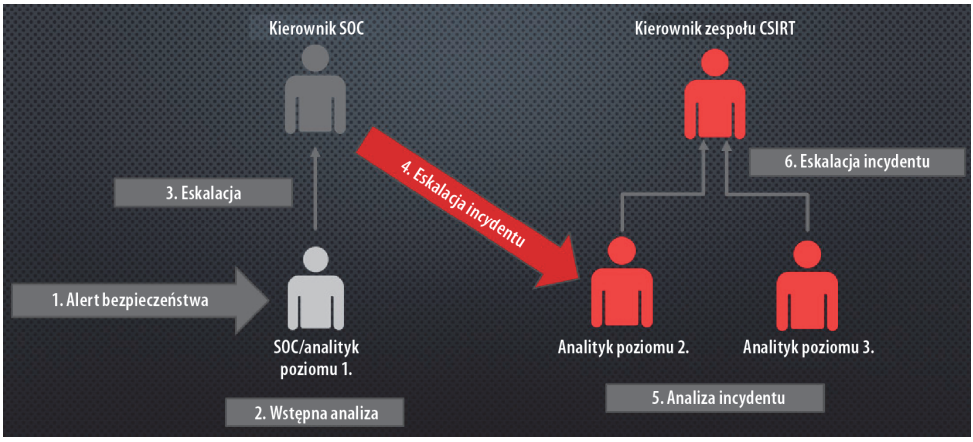
ROZDZIAŁ 1.
Czym jest reagowanie na incydenty

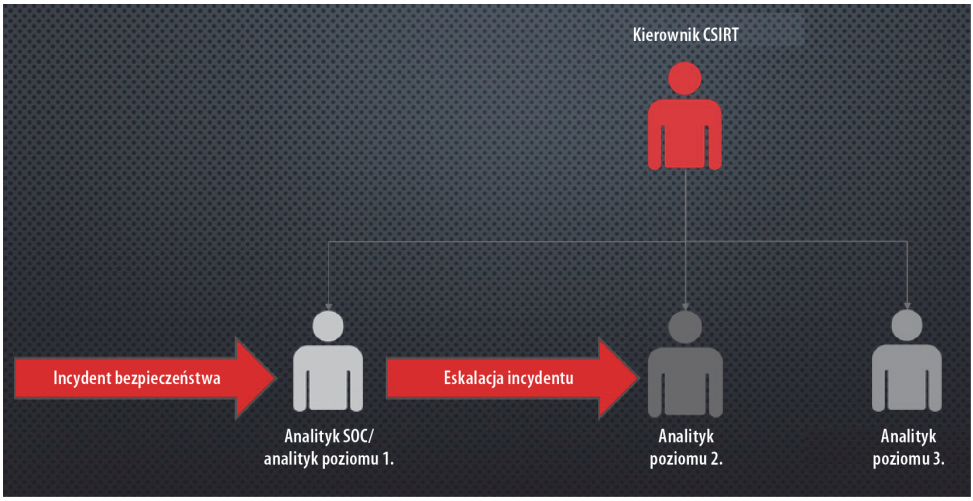


Rysunek 1.1. Proces reagowania na incydenty NIST

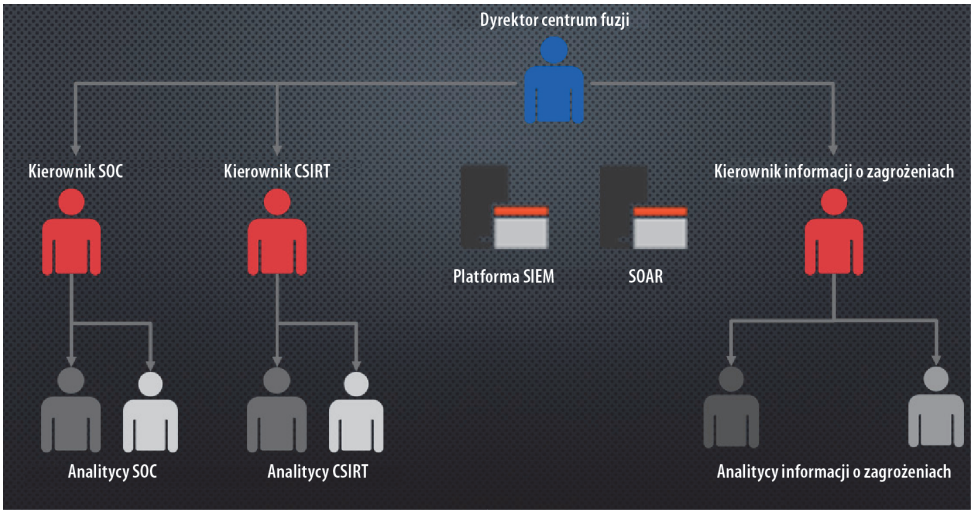
ROZDZIAŁ 2.
Zarządzanie incydentami cyberbezpieczeństwa



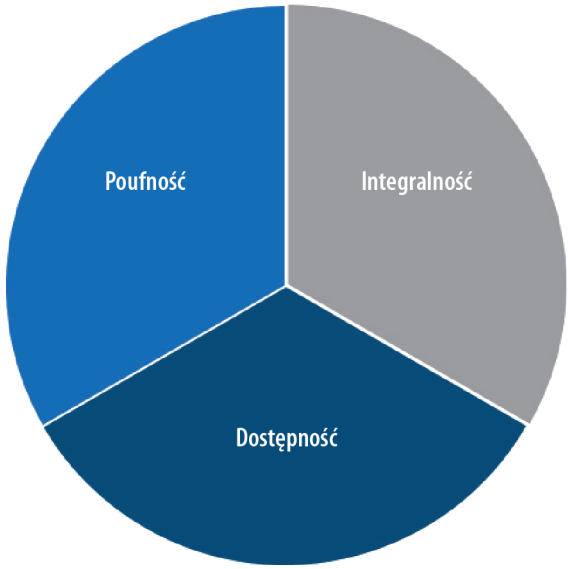
Rysunek 2.1. Model angażowania SOC



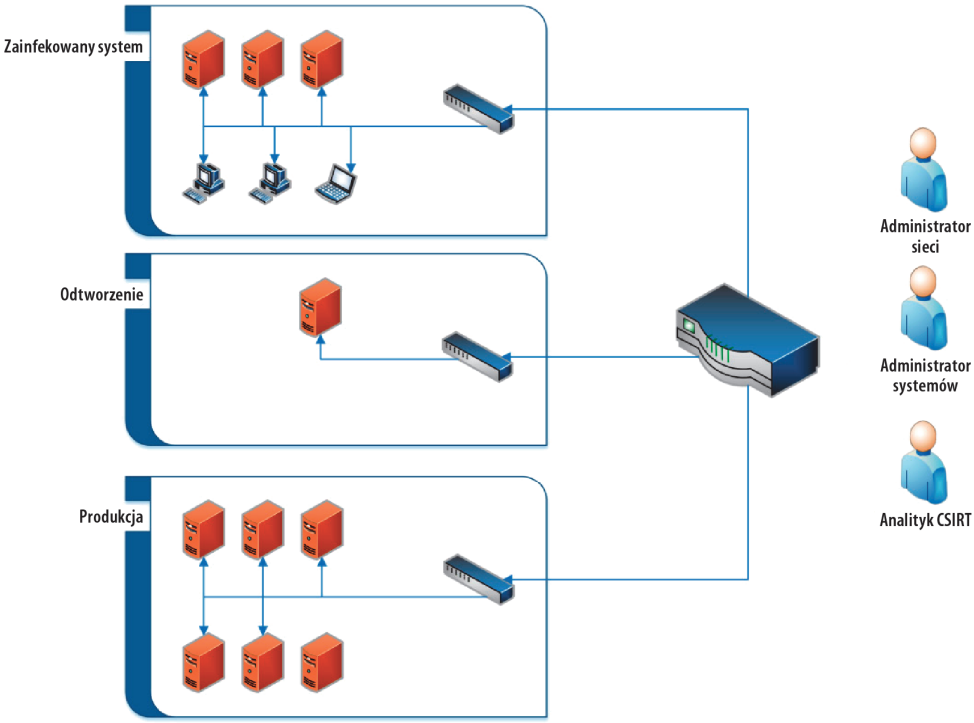
Rysunek 2.2. Zintegrowany model SOC



Rysunek 2.3. Model centrum fuzji

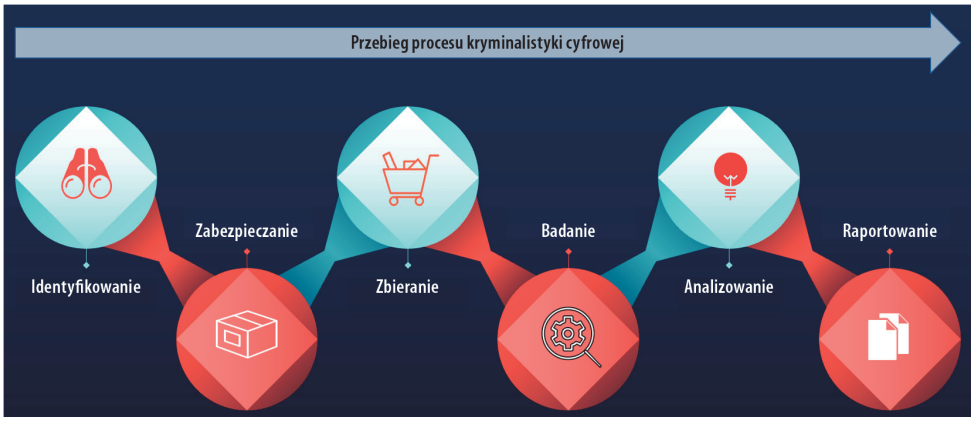


Rysunek 2.4. Triada CIA



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

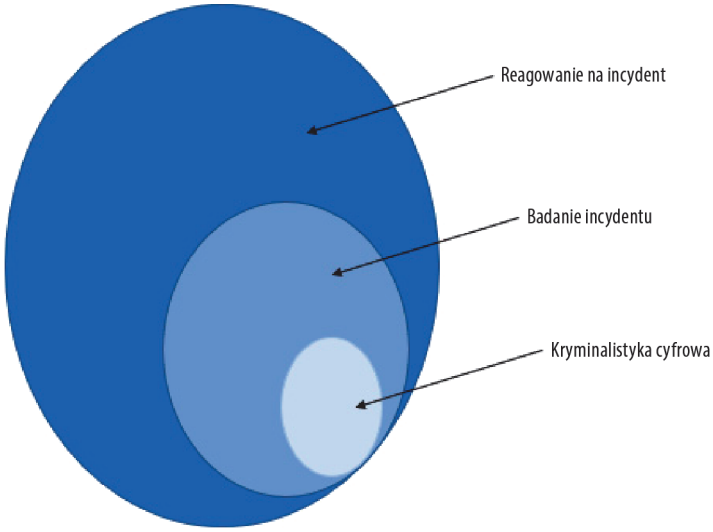
Rysunek 3.11. System operacyjny CSI Linux przeznaczony na potrzeby kryminalistyki cyfrowej

Rysunek 3.12. System operacyjny REMNUX przeznaczony na potrzeby kryminalistyki cyfrowej

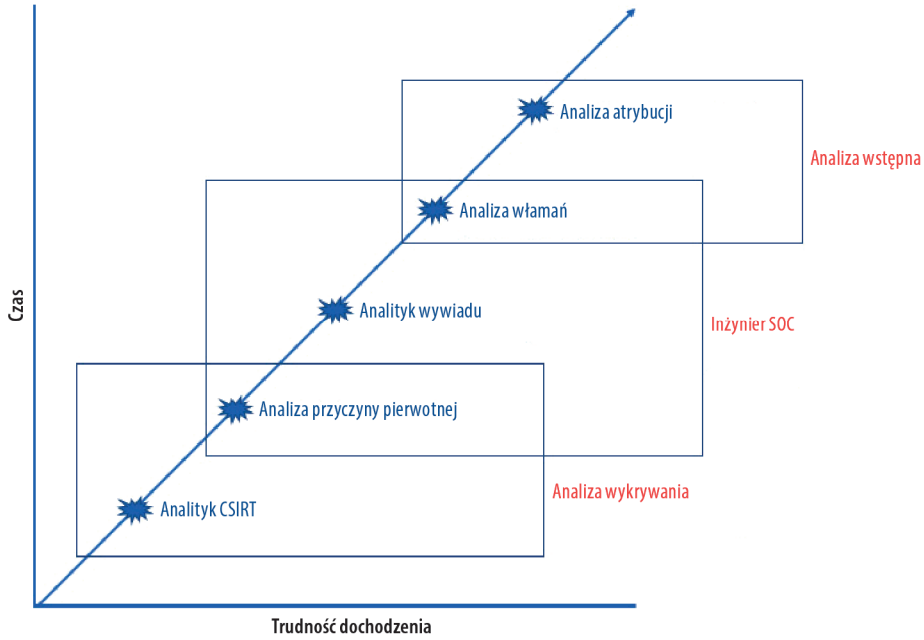
Rysunek 3.13. Zestaw przenośny do zastosowań w kryminalistyce cyfrowej

Rysunek 3.14. Zawartość zestawu przenośnego

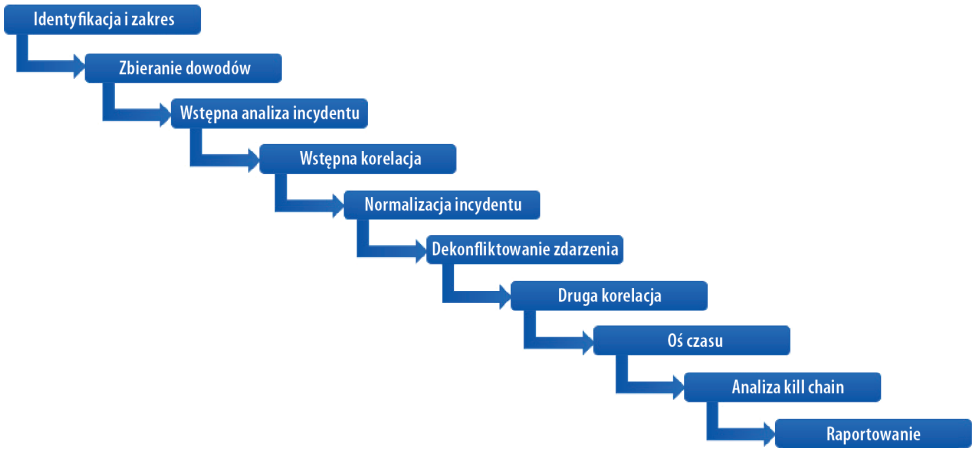
ROZDZIAŁ 4.
Metoda dochodzeniowa



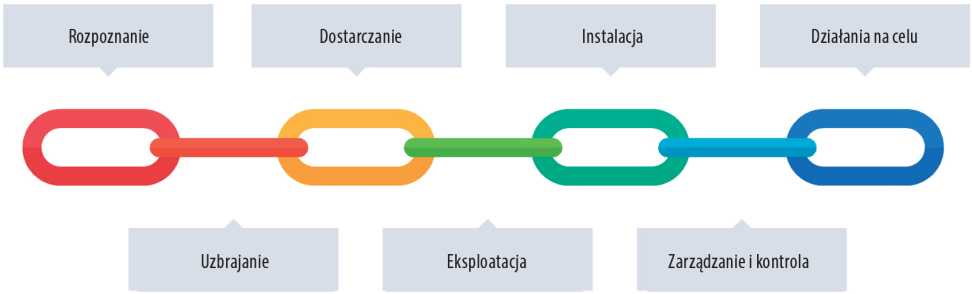
Rysunek 4.1. Związek między kryminalistyką cyfrową, badaniem incydentów a reagowaniem na incydenty



Rysunek 4.2. Rodzaje dochodzeń prowadzonych w sprawie incydentów cyfrowych

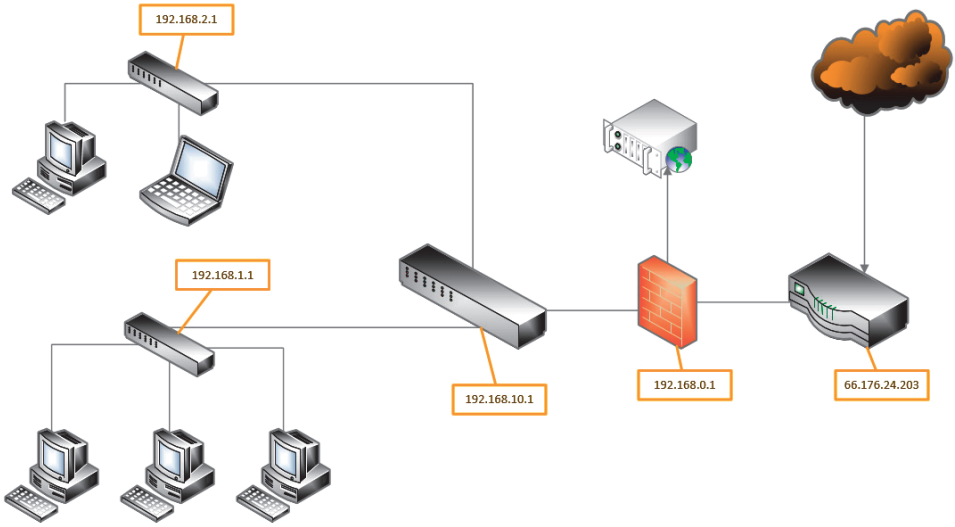


Rysunek 4.3. Dziesięcioetapowa metodyka dochodzenia

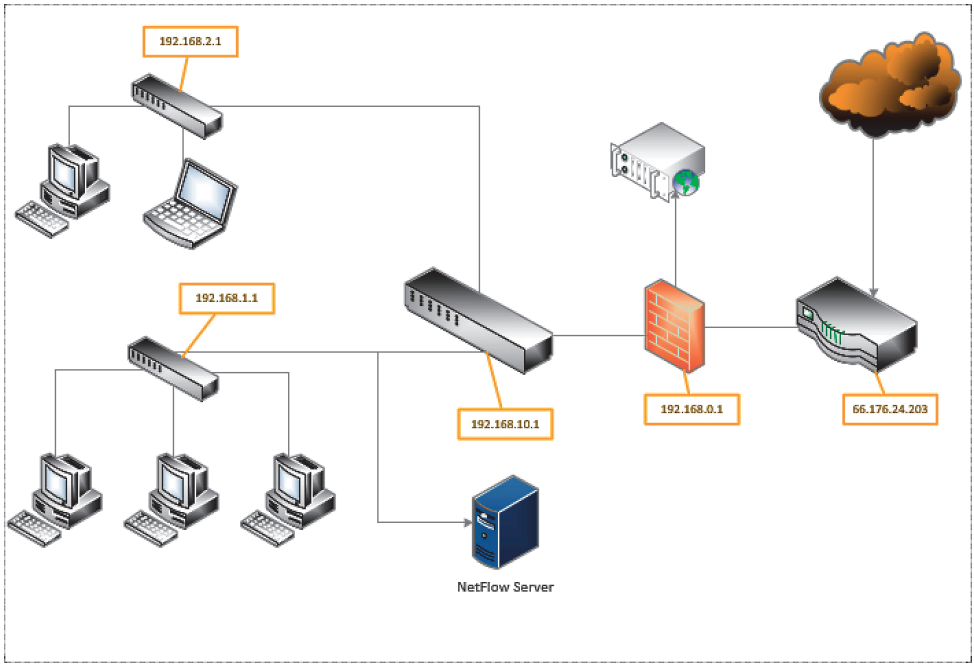


Rysunek 4.4. Łańcuch kill chain

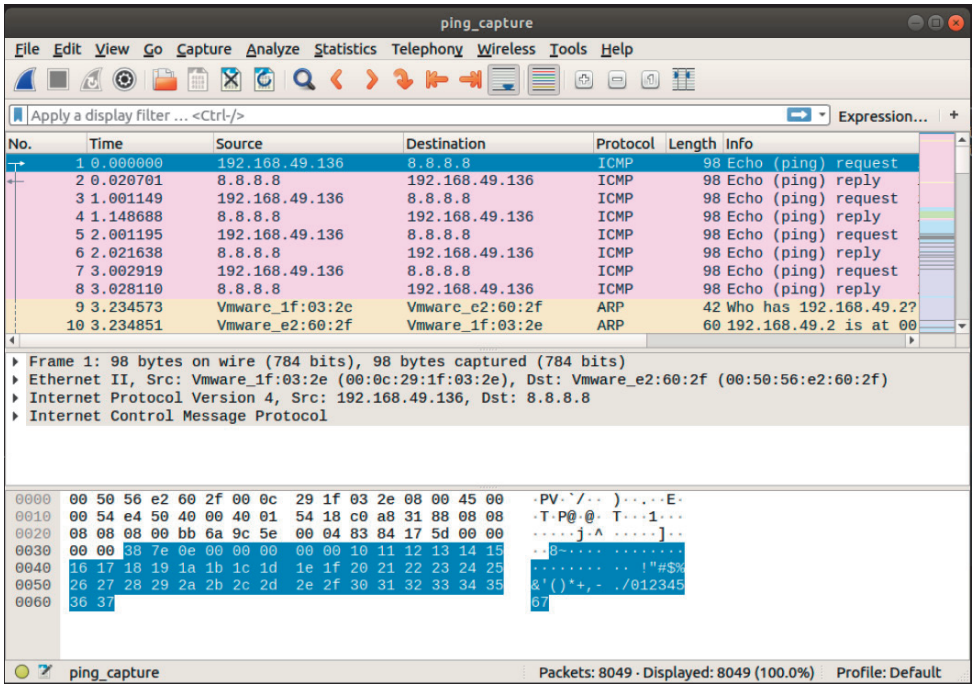
ROZDZIAŁ 5.
Zbieranie dowodów sieciowych



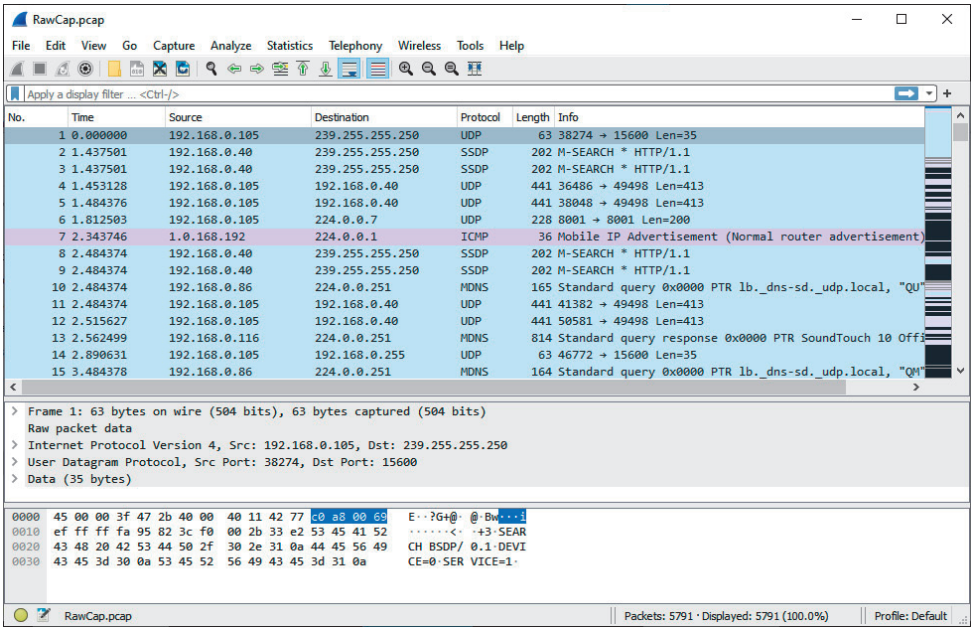
Rysunek 5.1. Przykładowy schemat sieci



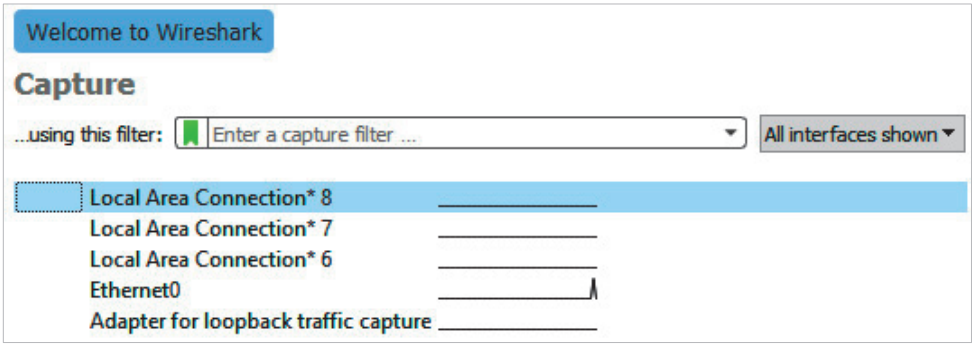
Rysunek 5.2. Diagram NetFlow



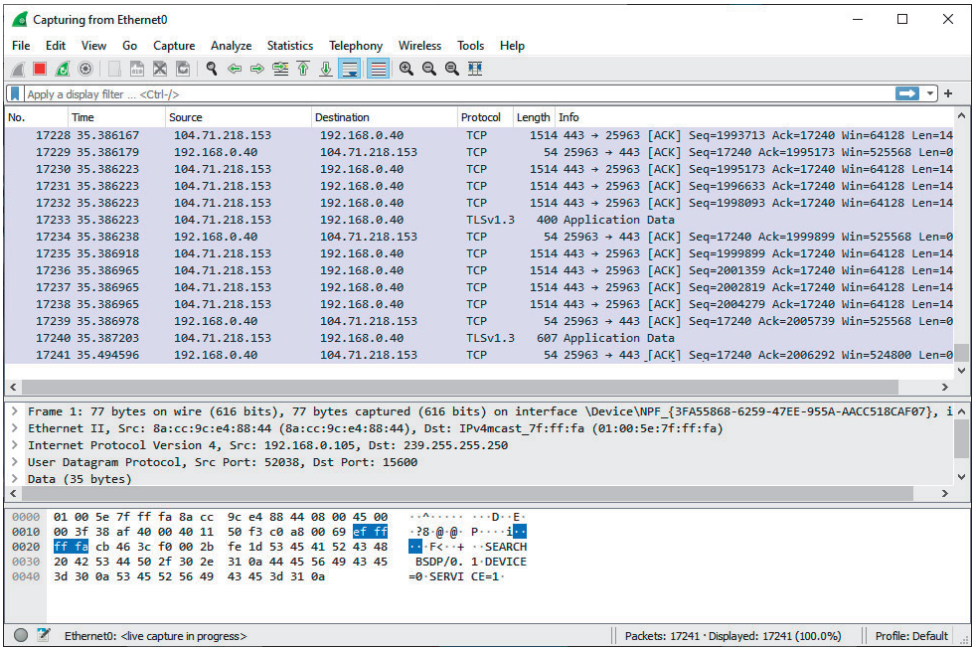
Rysunek 5.7. Analiza przechwytywanych pakietów w programie Wireshark



Rysunek 5.10. Analiza pliku RawCap w programie Wireshark

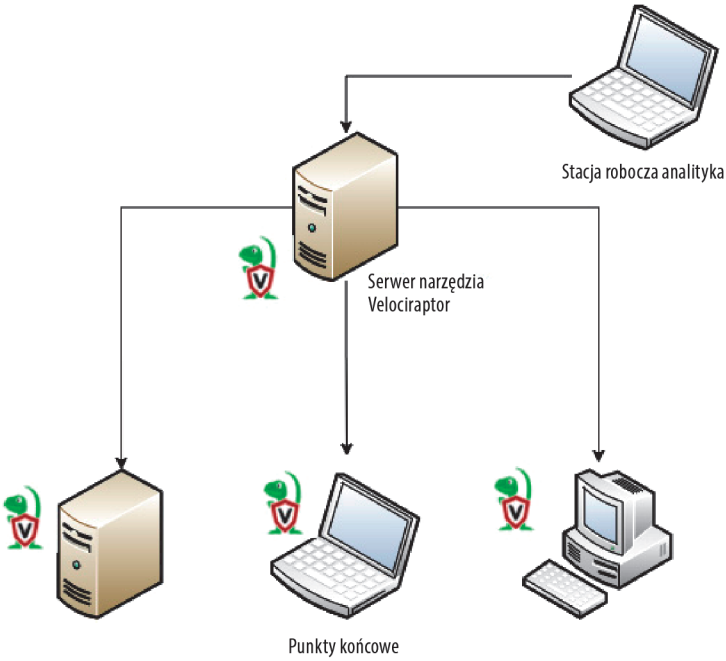


Rysunek 5.11. Interfejsy przechwytywania programu Wireshark



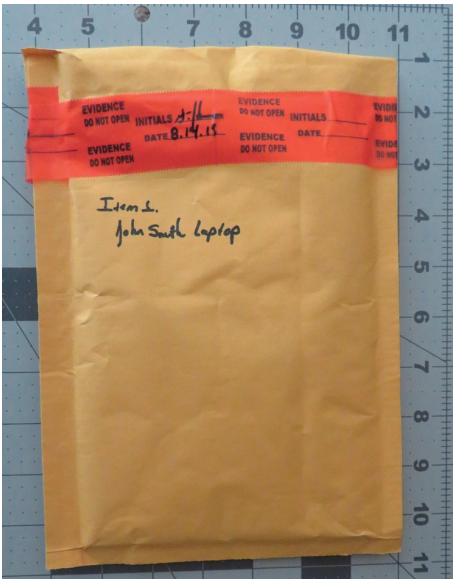
Rysunek 5.12. Widok przechwytywania programu Wireshark

ROZDZIAŁ 7.
Zdalne gromadzenie dowodów



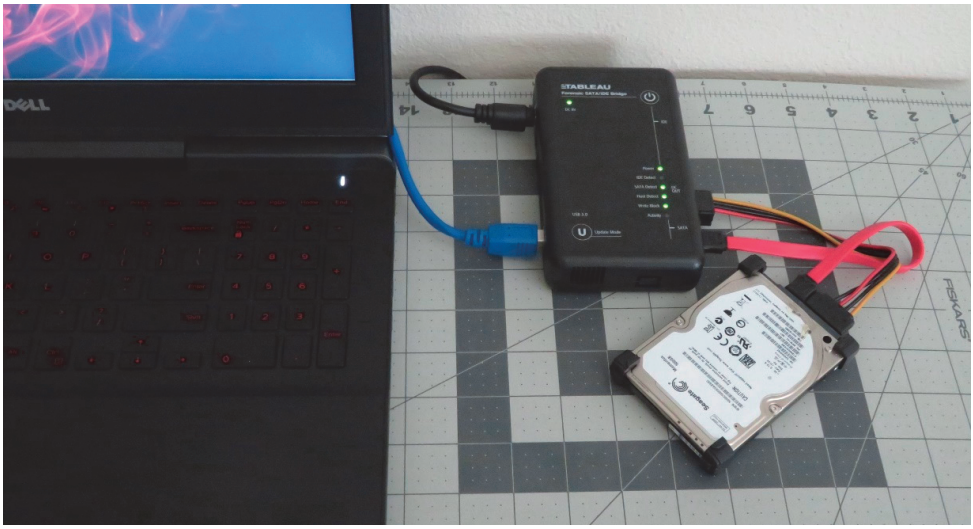
Rysunek 7.1. Konfiguracja narzędzia Velociraptor

ROZDZIAŁ 8.
Obrazowanie kryminalistyczne



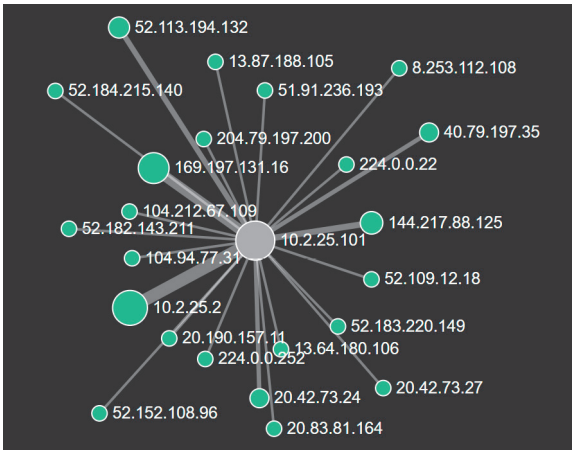
Rysunek 8.8. Kontrola integralności opakowania

Rysunek 8.9. Przykładowe zdjęcie dysku



Rysunek 8.10. Konfiguracja fizycznej blokady zapisu

ROZDZIAŁ 9.
Badanie dowodów sieciowych



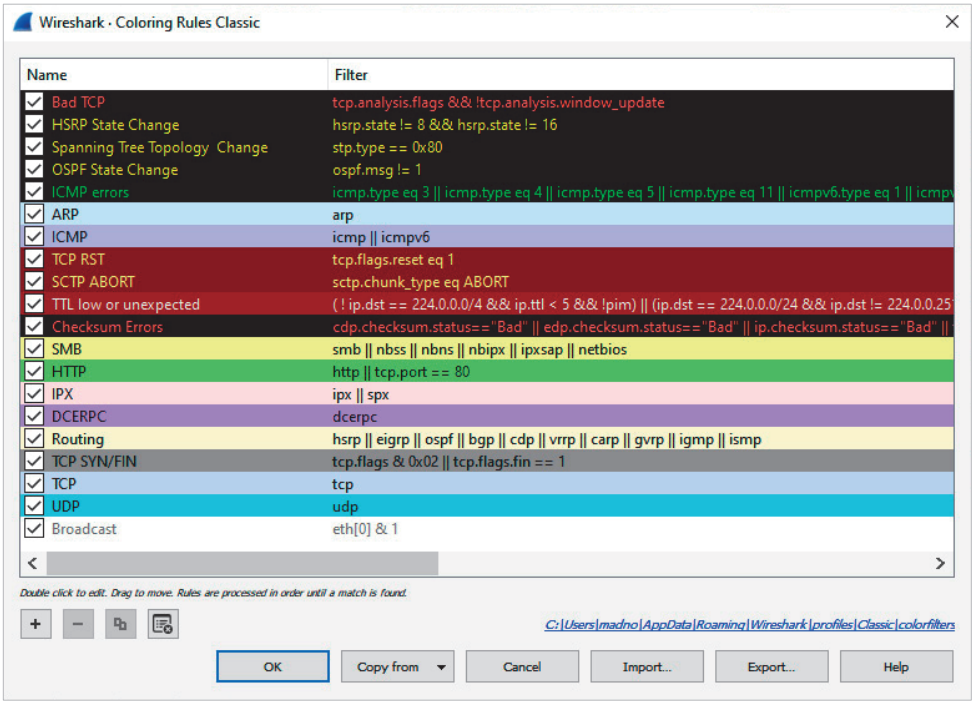
Rysunek 9.18. Wykres połączeń w Arkime

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

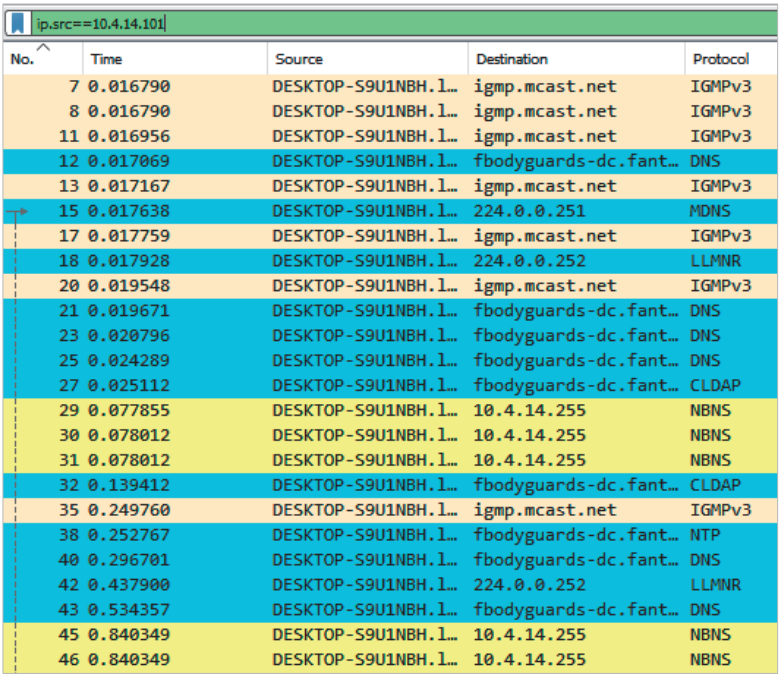
Rysunek 9.19. Widok adresów IP w narzędziu Wireshark

No.	Time	Source	Destination	Protocol
730	85.565098	204.79.197.219	DESKTOP-S9U1NBH.loc…	TCP
731	85.565098	DESKTOP-S9U1NBH.l…	204.79.197.219	TCP
732	85.565175	204.79.197.219	DESKTOP-S9U1NBH.loc…	TCP
733	85.565175	DESKTOP-S9U1NBH.l…	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.l…	204.79.197.219	TCP
737	85.611504	DESKTOP-S9U1NBH.l…	fbodyguards-dc.fant…	DNS
738	85.613032	DESKTOP-S9U1NBH.l…	204.79.197.219	TCP
739	85.895409	DESKTOP-S9U1NBH.l…	fbodyguards-dc.fant…	DNS
740	85.945248	fbodyguards-dc.fa…	DESKTOP-S9U1NBH.loc…	DNS
741	85.946784	DESKTOP-S9U1NBH.l…	geobram.com	TCP
742	86.108025	geobram.com	DESKTOP-S9U1NBH.loc…	TCP
743	86.108518	DESKTOP-S9U1NBH.l…	geobram.com	TCP
744	86.109239	DESKTOP-S9U1NBH.l…	geobram.com	HTTP
745	86.200705	DESKTOP-S9U1NBH.l…	239.255.255.250	SSDP
746	86.235023	DESKTOP-S9U1NBH.l…	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.l…	geobram.com	TCP
750	87.227980	DESKTOP-S9U1NBH.l…	geobram.com	HTTP
751	87.443277	geobram.com	DESKTOP-S9U1NBH.loc…	TCP

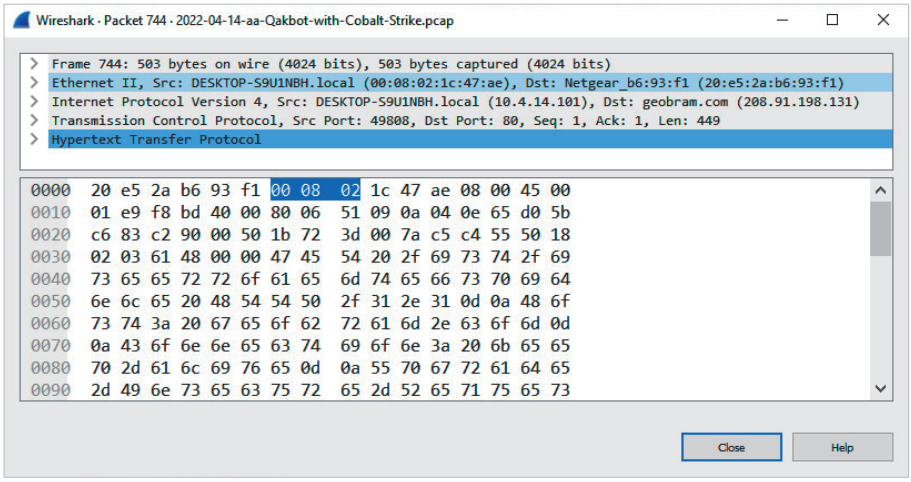
Rysunek 9.20. Widok nazwy domeny w Wiresharku



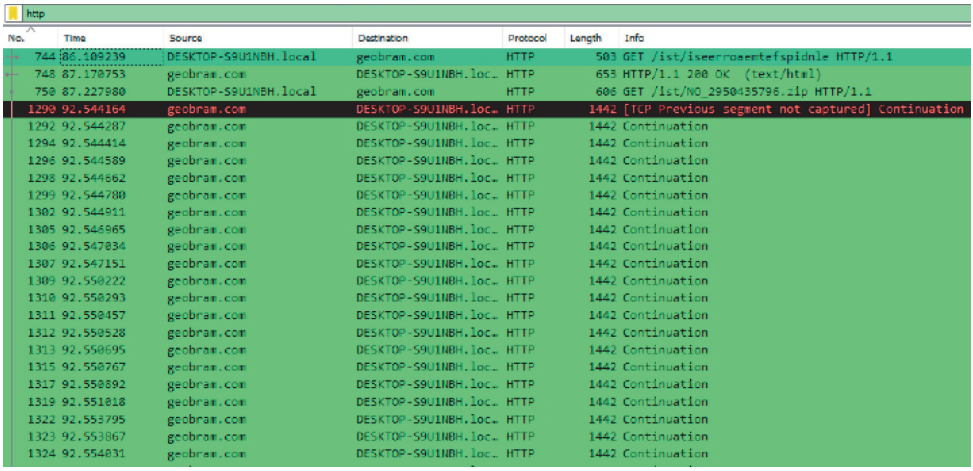
Rysunek 9.21. Klasyczne zasady kolorowania w Wiresharku



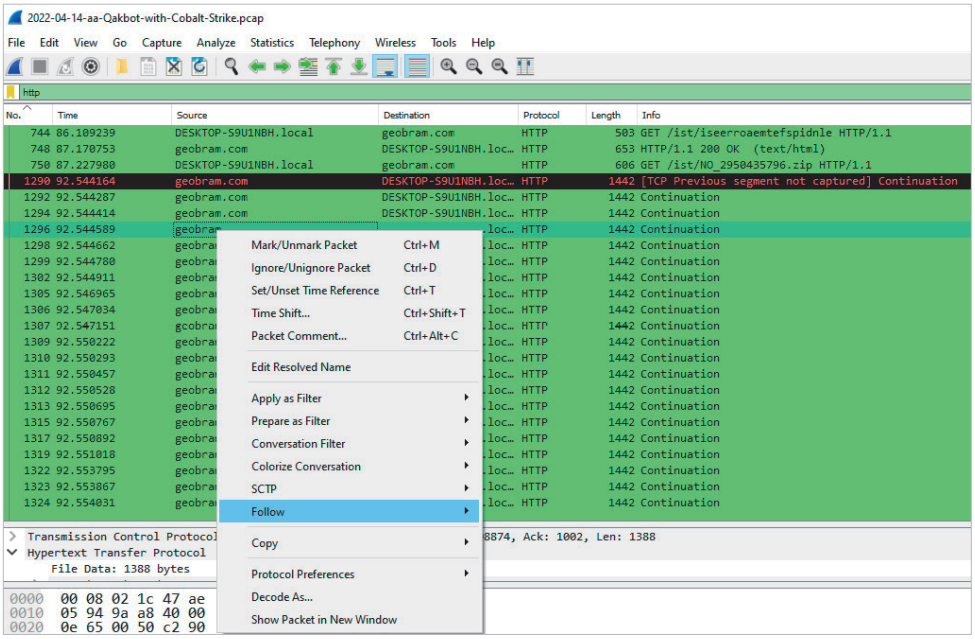
Rysunek 9.22. Filtrowanie po adresach źródłowych



Rysunek 9.23. Dane dotyczące pakietów

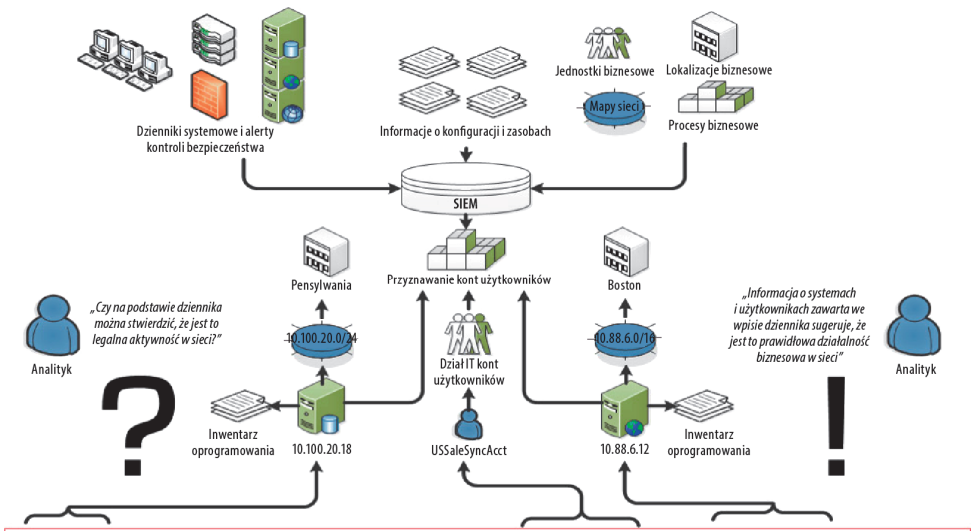


Rysunek 9.24. Widok pakietu HTTP



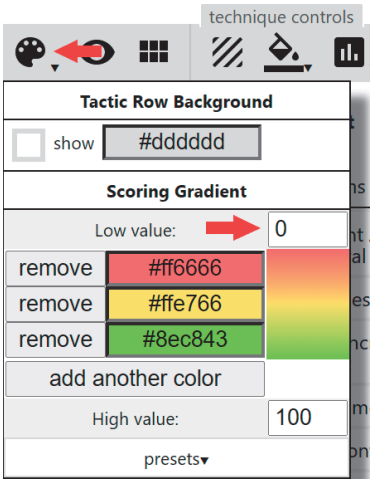
Rysunek 9.25. Śledzenie strumieni HTTP

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