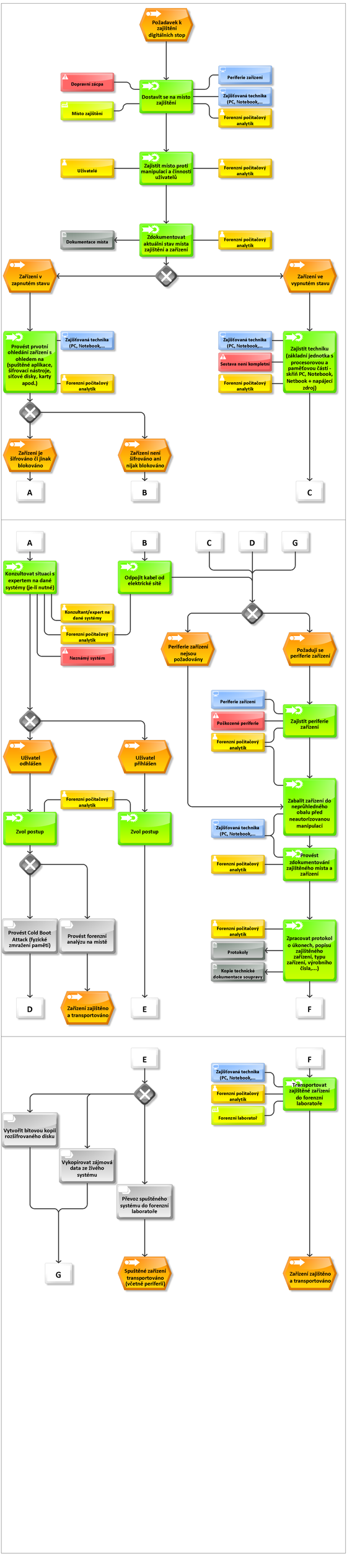
Požadavek k zajištění digitálních stop
Dopravní zácpa
Místo zajištění
Dostavit se na místo zajištění
Periferie zařízení
Zajišťovaná technika (PC, Notebook,...
Forenzní počítačový analytik
Uživatelé
Zajistit místo proti manipulaci a činnosti uživatelů
Forenzní počítačový analytik
Dokumentace místa
Zdokumentovat aktuální stav místa zajištění a zařízení
Forenzní počítačový analytik
Zařízení v zapnutém stavu
Zařízení ve vypnutém stavu
Provést prvotní ohledání zařízení s ohledem na (spuštěné aplikace, šifrovací nástroje, síťové disky, karty apod.)
Zajišťovaná technika (PC, Notebook,...
Forenzní počítačový analytik
Zajišťovaná technika (PC, Notebook,...
Sestava není kompletní
Forenzní počítačový analytik
Zajistit techniku (základní jednotka s procesorovou a pamětovou části - skříň PC, Notebook, Netbook + napájecí zdroj)
Zařízení je šifrováno či jinak blokováno
Zařízení není šifrováno ani nijak blokováno
A
B
C
A
B
C
D
G
Konzultovat situaci s expertem na dané systémy (je-li nutné)
Konzultant/expert na dané systémy
Forenzní počítačový analytik
Neznámý systém
Odpojit kabel od elektrické sítě
Periferie zařízení nejsou požadovány
Požadují se periferie zařízení
Periferie zařízení
Poškozené periferie
Forenzní počítačový analytik
Zajistit periferie zařízení
Uživatel odhlášen
Uživatel přihlášen
Forenzní počítačový analytik
Zvol postup
Zvol postup
Zabalit zařízení do neprůhledného obalu před neautorizovanou manipulací
Zajišťovaná technika (PC, Notebook,...
Forenzní počítačový analytik
Provést zdokumentování zajištěného místa a zařízení
Provést Cold Boot Attack (fyzické zmražení paměti)
Provést forenzní analýzu na místě
Forenzní počítačový analytik
Protokoly
Kopie technické dokumentace soupravy
Zpracovat protokol o úkonech, popisu zajištěného zařízení, typu zařízení, výrobního čísla,...)
D
Zařízení zajištěno a transportováno
E
F
E
F
Zajišťovaná technika (PC, Notebook,...
Forenzní počítačový analytik
Forenzní laboratoř
Transportovat zajištěné zařízení do forenzní laboratoře
Vytvořit bitovou kopii rozšifrovaného disku
Vykopírovat zájmová data ze živého systému
Převoz spuštěného systému do forenzní laboratoře
G
Spuštěné zařízení transportováno (včetně periferií)
Zařízení zajištěno a transportováno